行政院國家科學委員會專題研究計畫　成果報告

應用自我組織映射網路於網路入侵偵測之研究

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-034-003-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：中國文化大學資訊管理學系暨研究所

計畫主持人：蔡敦仁

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 92 年 10 月 6 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

應用自我組織映射網路於網路入侵偵測之研究

計畫類別：☑ 個別型計畫 □ 整合型計畫
計畫編號：NSC 91－2213－E －034－003－
執行期間： 91 年 8 月 1 日至 92 年 7 月 31 日

計畫主持人：蔡敦仁
共同主持人：戴文彬
計畫參與人員： 張繼方、林惠徵

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
□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：私立中國文化大學資訊管理系

中 華 民 國 92 年 9 月 30 日

應用自我組織映射網路於網路入侵偵測之研究

A Study of Network Intrusion Detection Using Self-Organization Network

一、中文摘要

目前入侵偵測上使用的偵測方式可分為不正常行為偵測法(abnormal detection)與入侵定義偵測法(misuse detection)兩種，但不論是採取哪種偵測法都會有先天上的限制，如無法發現新型的入侵行為、錯誤入侵警告(false alarm)等缺點。因此為了使此兩種偵測方式能相互並存以達到相互輔助的效益，在這提出應用類神經網路中的自我組織映射(self-organization map)方法來合併此兩種偵測方式，能偵測已知攻擊模式中的同時又可發現新的攻擊模式的系統架構。本計畫將以偵測阻絕服務攻擊來驗證所提出的入侵偵測模式。並使用模糊專家系統(fuzzy expert system)與倒傳遞網路(back-propagation network)架構對未知的行為模式重新訓練調整之後做出正確判斷。

關鍵詞:入侵偵測、自我組織映射、類神經網路、不正常行為偵測法、入侵行為定義偵測法、模糊專家系統、倒傳遞網路

ABSTRT

There are two intrusion detection approaches, abnormal detection and misuse detection. Abnormal detection and misuse detection have their own limitations. For example, misuse detection can't discover new type of intrusions, abnormal detection causes false alarm and so on. In order to make the two approaches complement each other, we apply self-organization map to combine abnormal detection with misuse detection. The new intrusion detection model would detect known intrusion behavior patterns and discover unknown intrusion simultaneously. The study concentrates on detecting denial of service to verify the new intrusion detection model. Then, we apply fuzzy expert system and back-propagation model to make more accurate judgements after re-trained with unknown intrusions.

Keyword: intrusion detection、self-organization map、abnormal detection、misuse detection、fuzzy expert system、back-propagation network

二、緣由與目的

在今日網際網路中資料竊取、阻絕服務等駭客攻擊行為不斷發生情況下，已有許多安全防護上的機制作安全防衛的動作[3][4]，而入侵偵測系統（intrusion detection system）在整個資訊安全的體系下是扮演警衛的角色，主要工作是偵測入侵事實的發生。目前使用入侵偵測的方式中可分為不正常行為偵測法（abnormal detection）與入侵行為定義偵測法（misuse detection）兩類，不正常行為偵測法是先對正常使用者行為特徵作定義，當有不符合正常使用者行為特徵時，就表示

可能有入侵行為發生，其優點是可找出新型的攻擊行為特徵；相反地，入侵行為定義偵測法是先對入侵者行為特徵先定義，當有符合入侵者行為特徵時就表示入侵行為發生了，其優點是入侵偵測的準確度高。

雖然此兩種偵測法都有其優點，但也有其缺點；不正常行為偵測法的缺點是容易產生錯誤的入侵警告（false alarm），而入侵定義偵測法的缺點是不容易發現未知攻擊行為特徵[9][11]。

不論採用不正常行為偵測法或入侵行為定義偵測法都會有所缺失，顧此失彼；因此如何在此兩種分析方法中找出折衷的地方，使其既能減少錯誤警告訊息的同時又能動態偵測出未知的新型攻擊特徵是本計畫主要的目標。本計畫主要是採取自我組織映射法來結合不正常行為偵測法與入侵行為定義偵測法，以達到互補的效果。並使用模糊專家系統與倒傳遞網路架構對未知的行為模式重新訓練調整之後做出正確判斷。

2.1 入侵偵測的分析方法

不論在不正常行為偵測法或是入侵行為定義偵測法中，主要偵測的方式不外是將原始資料作分析判斷，目前分析方法大致包含下列幾種統計分析法、模糊網路（fuzzy network）、規則設計分析（rule-based approach）、狀態轉換分析（state transition approach）、貝氏網路分析（bayesian network）等[1][12]。本計畫著重在用類神經網路分析的入侵偵測模式。

2.2 類神經網路在入侵偵測上的應用

類神經網路優於其他分析方法之好處在於，一.平行處理，執行處理能力效率高。二.錯誤容忍度，不需要完整的資料就可分析。三.學習能力，能隨著外在環境的變化而有所調適[2]。以上優點使類神經網路在使用者行為不定性與需快速偵測反應的入侵偵測的應用上十分適用。但相對的類神經網路在入侵偵測上的應用也有其缺點，如網路訓練時間長、對侵入行為的發生現象無法解釋、容易發生 false alarm 等缺點，這些都是本計畫要克服的問題。

目前已有若干文獻提出類神經網路應用在入侵偵測的實行，如 Bonofacio, Cansian 及 Carvalho (1998)[7]將入侵偵測模式分為階層式，由一層一層來過濾資訊，最後再交由倒傳遞網路分析。其入侵偵測模式重點在於先利用專家系統將網路上所擷取的封包資訊設定安全等級(security level)，如假設 finger 指令安全等級為 10，telnet 安全等級為 15，當 A 機器向本地主機發出 finger 指令，A 機器的安全等級為 10，當 A 機器又向本地主機發出 telnet 指令時，A 機器的安全等級要再加 15，一共為 25，而來源機器安全等級越高表示越是可疑。再交由語意分析器(semantic analyzer)從封包資料中找出可疑的指令字串，如 root、passwd 等指令字串。其輸入向量變數為六個，服務能力等級(service capacity level)、服務鑑別等級(service authentication level)、來源及目的主機安全等級(security level of the source and destination machine)、傳輸資料容量大小(quantity of transferred data)、連接時間(connect time)、可疑字串個數(the amount of suspicious strings)。

Debar, Becker 及 Siboni (1992)[5]則是將倒傳遞網路與專家系統合併運用，首先是將類神經

網路運用在分析使用者不定性的行為模式，使其對使用者的行為特徵能更完美的表達，接者再將類神經網路所分析出的數值資訊轉換為符號交由專家系統做決策，由專家系統的知識庫中來判斷是否符合入侵行為的特徵。

Lippmann 及 Cunningham (2000)[10]則是將倒傳遞網路與自我組織映射網路運用在增進關鍵字偵測(keyword selection)入侵偵測的效率上，以往關鍵字偵測的缺點在於常發生錯誤警告，把正常行為誤判為攻擊行為的發生。所以此研究將一般常用的關鍵字(generic keywords)與特定的攻擊關鍵字合併做分析，而此研究主要是運用兩個類神經網路，一個是用來偵測估計攻擊可能發生的機率；一個是用來區分已知的攻擊模式類別，以便知道當發生攻擊時是哪一種類型的攻擊模式。

Girardin (1999)[8]主要是將自我組織映射網路運用在網路流量的入侵偵測測分析上，此研究將網路中所擷取的封包資料交給自我組織映射網路做分析，發現每個不同協定或同協定而不同時間特性的封包特性可做資料分類，藉此再延伸出對攻擊封包資料作分析與分類，以達到入侵偵測的應用，其輸入向量變數為 8 個，分別為時間郵戳(time stamp)、IP 來源位置與目的位置、來源埠與目的埠(source port and destination port)、封包序列編號(sequence number)、封包容量大小(packet size)、封包長度(packet length)、緊急旗標(urgent flag)。

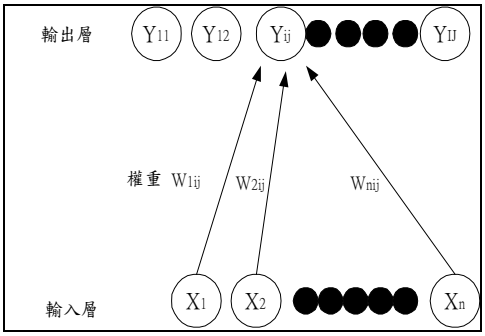
另外 Dickerson 及 Dickerson (2000)[6]則是將模糊網路(fuzzy network)運用在網路的入侵偵測應用，首先是利用網路資料處理單元(network data processor)將從網路上所攫取到的封包資料作初步資料挖掘的動作，將原始封包資料轉換為整理過的統計數據，再將這些統計數據交由模糊網路做入侵偵測的分析。其中比較特別的設計變數就是 sdp，所謂 sdp 就是將 IP 來源位置、IP 目的位置與目的埠(destination port)合併一起，用來表示有兩台主機間有 TCP 協定服務的存在，其輸入向量變數為 8 個，分別為在封包收集的單位時間內所擷取到的封包總個數、在封包收集的單位時間內所監測的 sdp 總個數、在封包收集的單位時間內所擷取到新的 sdp 個數、以前從未見過而第一次出現的 sdp 個數、已知的服務埠(service port)出現的個數、來源位置為網路外的 IP 位置之 sdp 個數、成功建立 TCP 協定溝通的個數、已觀察過之封包個數與 sdp 個數間的變異數。

由上述研究、文獻中我們發現入侵偵測模式有些是偏向不正常行為偵測法，不然就是偏向入侵行為定義偵測法，會有顧此失彼的現象發生，無法避免此兩種偵測法運用上的缺點；而其中在 Girardin (1999)的研究中主要是將自我組織映射網路運用在網路流量的入侵偵測測分析上，並無特別強調可運用自我組織映射將不正常行為偵測法與入侵行為定義偵測法合併，因此所達到的偵測效果有限，所以在本計畫中將以阻絕服務攻擊為研究樣本範圍來證明自我組織映射網路可以達到結合此兩種偵測法的優點。

2.3 自我組織映射（self-organization map）

自我組織映射是屬於一種無監督式學習網路模式，它模仿人腦有不需教導就可將具有相似特性的事物歸類成一類的特性，而藉由輸入變數來作分析，而不需事先告與資料所屬的類別，當網路學習完成時，其輸出處理單元有相似特徵者會自我匯集，產生叢聚(cluster)的現象，以達成資料挖掘(data mining)的效益[13]，此分析方法與統計學上的叢聚分析的原理相似，目前自我組織映射分析方法主要應用在語音與圖像辨識的處理上，在往後的章節裡我們說明如何將自我組織映射結合不正常行為偵測法與定義入侵行為偵測法，在此以 Kohonen 所提的自我組織架構為基礎

來延伸，其整體網路架構圖如圖一所示：



圖一：Kohonen 的自我組織映射網路架構

三、研究方法

3.1 研究樣本

本計畫的研究範圍限制在針對阻絕服務的攻擊，資料來源的取得是藉由封包監聽程式(sniffer)收集阻絕服務攻擊程式所產生的封包資料，我們將所收集的攻擊封包資料可分為 ICMP 協定、UDP 協定、TCP 協定此三類，本計畫中所收集的阻絕服務攻擊共有六個程式，另外本計畫還對正常行為模式封包資料作定義。

(一)ICMP 協定

1. bloop 攻擊程式

攻擊端使用假 IP 來源不斷對目的主機發出 ICMP 協定的 echo reply 與 param_probl 之封包，來消耗目的主機對外連線的頻寬。

2. xicmp 攻擊程式

攻擊端不斷對目的主機發出 ICMP 協定的 echo request 封包，使目的主機忙於回應攻擊端的請求而不斷回應 ICMP 的 echo reply 封包，來消耗目的主機的系統資源。

(二)UDP 協定

1. panther 攻擊程式

攻擊端不斷對目的主機發出 UDP 協定的封包請求，使目的主機忙於回應攻擊端的請求而不斷回應 ICMP 協定的目的位置無法到達之回應(destination unreachable)，來消耗目的主機的系統資源。

2. overdrop 攻擊程式

攻擊端利用假的不同 IP 位置不斷對目的端發出 UDP 協定之封包，藉此來消耗目的主機對外連線的頻寬。

3. rc8 攻擊程式

攻擊端利用假的唯一 IP 位置不斷對目的端發出不斷對目的端發出 UDP 協定之 echo 回應封包，藉此來消耗目的主機對外連線的頻寬。

(三)TCP 協定

1. synk4 攻擊程式

攻擊端利用假的不同 IP 來源位置不斷對目的端發出 TCP 協定的 HTTP 請求封包，將目的端的等待佇列佔滿，使目的主機無法，對合法的正常使用請求回應，甚至會導致目的端主機癱瘓。

(四)正常行為封包資料

由於本計畫是利用自我組織映射網路來結合入侵行為模式定義之偵測與不正常行為模式之偵測，所以資料來源除了前文說明之六種阻絕服務攻擊封包資料之外，還需定義正常行為模式之封包資料，在此定義正常行為模式為允許內部網路 IP 對外部網路實行 HTTP 協定。

本計畫以每單位時間 5 秒將所收集的封包資料作整理，而各攻擊程式所整理出的資料筆數整理如表一所示。

表一 單位時間 5 秒輸入變數資料筆數統計

攻擊程式	資料樣本筆數
bloop 攻擊程式	120 筆
xicmp 攻擊程式	256 筆
panther 攻擊程式	277 筆
overdrop 攻擊程式	386 筆
rc8 攻擊程式	91 筆
Synk4 攻擊程式	254 筆
正常行爲封包資料	331 筆
總計	1715 筆

3.2 輸入變數

本計畫的研究範圍主要是針對阻絕服務攻擊的封包資料作分析，因此篩選的輸入變數要反映出阻絕服務攻擊的資料特性，以供類神經網路分析，選取的輸入變數為單位時間內的封包資料之統計整理，在研究中共設計八個計量指標，分別說明如下。

(一)unicip_ac

在單位時間內當來源 IP 位置屬於外部網路的 IP 位置時，且來源 IP 位置為第一次出現的 IP 位置時，便做次數計量的動作。若此指標變數高，表示有許多不同外部來源 IP 位置出現；相對的，若此指標變數低，表示只有一個外部來源 IP 位置出現。

(二)unicportsrc_ac

在單位時間內當來源埠(source port)為第一次出現的來源埠序號時，便做次數計量的動作。若此指標高，表示外部的來源機器以不同的來源埠對目的主機通訊；相對的，若此指標變數低，表示來源機器以唯一的來源 por 對目的主機通訊。

(三)unicportdest_ac

在單位時間內當目的埠(destination port)為第一次出現的目的埠序號時，便做次數計量的動作。若此指標高，表示外部的來源機器對目的主機不同目的埠通訊；相對的，若此指標變數低，表示來源機器對目的主機唯一的目的 port 通訊。

(四)udp_ac

在單位時間內當擷取到 UDP 封包時，便做次數計量的動作。若此指標高，表示來源端主機對目的主機發出大量的 UDP 封包流量。

(五)icmp_ac

在單位時間內當擷取到 ICMP 封包時，便做次數計量的動作。若此指標高，表示來源端主機對目的主機發出大量的 ICMP 封包流量。

(六)tcp_ac

在單位時間內當擷取到 TCP 封包時，便做次數計量的動作。若此指標高，表示來源端主機對目的主機發出大量的 TCP 封包流量。

(七)inip_ac

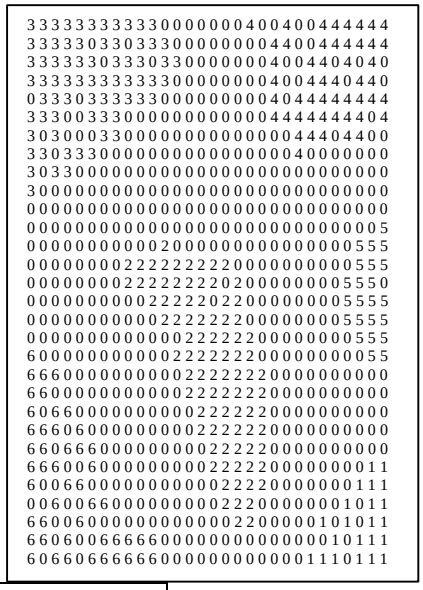
在單位時間內當來源 IP 屬於內部網路的 IP 位置時，便做次數計量的動作。若此指標高，表示目的主機忙於回應網路外部機器的封包請求。

(八)inter_total

在單位時間當攫取到封包時，便做次數計量的動作

四、結果與討論

先將各個攻擊程式所產生的封包資料做資料分類標示的動作，以供辨識網路訓練後的樣本資料叢集範圍，而封包資料的分類標示如表二與三所示，表二為訓練樣本資料的分類，表三為測試範例樣本資料的分類。



攻擊程式	類別
bloop 攻擊程式	第 1 類
xicmp 攻擊程式	第 2 類
panther 攻擊程式	第 3 類
overdrop 攻擊程式	第 4 類
rc8 攻擊程式	第 5 類
正常行爲封包資料	第 6 類

表二　訓練樣本資料的分類

表三　測試樣本資料的分類

攻擊程式	類別
正常行爲模式測試封包資料	第 7 類
synk4 攻擊程式	第 8 類
overdrop 測試攻擊程式	第 9 類

其中將正常行為模式測試封包資料分為第 7 類，是為了表示為新的已知正常行為模式封包資料，主要是測試正常行為模式在自我組織映射網路上的辨識效果；synk4 攻擊程式分為第 8 類，是為了表示為網路未訓練的輸入樣本變數，主要是測試自我組織映射網路在不正常行為模式之偵測的效果；overdrop 測試攻擊程式分為第 9 類是為了表示為新的已知攻擊程式，主要是測試入侵行為定義之偵測的效果。

當經由資料分類後，再分別以單位時間 5 秒將樣本資料轉換為輸入變數資料，接著將輸入變數交由自我組織映射網路來調整與學習，最後以 30×30 的網路拓樸矩陣來呈現資料的叢聚情形，以單位時間 5 秒訓練輸入樣本資料在自我組織映射網路的網路拓樸所呈現的結果如圖二所示。

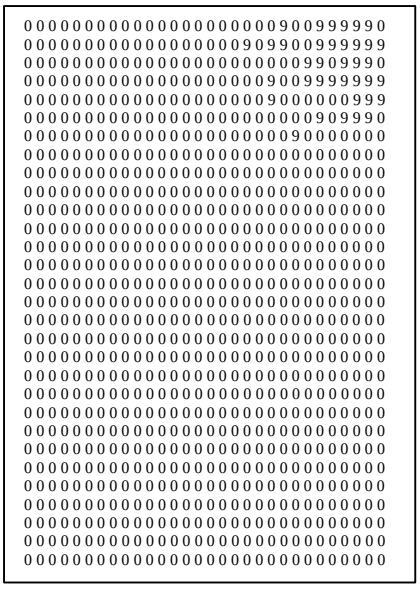
圖二 單位時間 5 秒訓練樣本資料在網路拓樸呈現之結果

我們可以知道以單位時間 5 秒的輸入樣本資料在 30×30 的網路矩陣拓樸中都呈現明顯的叢集(cluster)現象。藉由資料在網路拓樸上叢集的特徵，本計畫以自我組織映射網路所分析後的網路矩陣拓樸為基礎，來實行結合入侵行為模式定義之偵測與不正常行為模式之偵測的研究目的。

4.1 自我組織映射網路在入侵行為定義偵測的分析結果

本計畫以自我組織映射網路分析後的網路拓樸為基礎做入侵偵測上的應用，藉由訓練後的網路權重資料來達成測試範例在網路拓樸上的落點，將訓練範例所形成的網路拓樸與測試範例所形成的網路拓樸相互比對分析，來達到入侵偵測的效果，分析後的資料叢集範圍如圖三所示。

第 9 類的 overdrop 測試攻擊程式用來測試已知的第 4 類 overdrop 攻擊程式在入侵行為模式定義偵測，我們以訓練後已知的網路拓樸來做已知攻擊資料作分析比對，衡量訓練後的網路拓樸在已知的入侵攻擊行為模式的效果，研究中發現有 0.865 的偵測準確度。

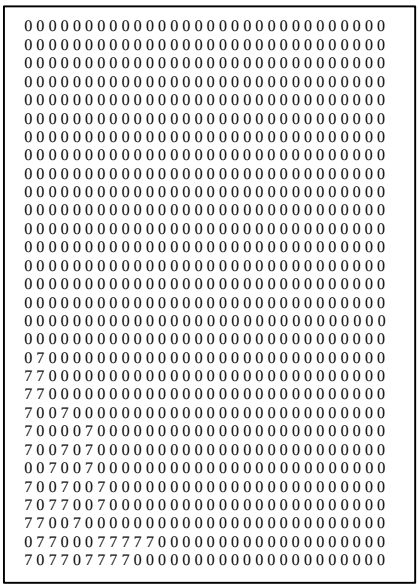


圖三　類別 9 單位時間 5 秒測試範例在網路拓樸呈現結果

4.2 自我組織映射網路在正常行為模式定義偵測的分析結果

本計畫的自我組織映射網路入侵偵測模式除了要達到入侵行為模式定義之偵測外，同時還要達到不正常行為模式之偵測的效果，因此在訓練範例中另外加入了正常行為模式定義之資料，定義使用者之正常行為模式，偵測合法的使用者行為，當有分析後的資料落點在正常行為模式的落點範圍內，就表示為合法的使用者行為產生，分析後的資料叢集範圍如圖四所示。

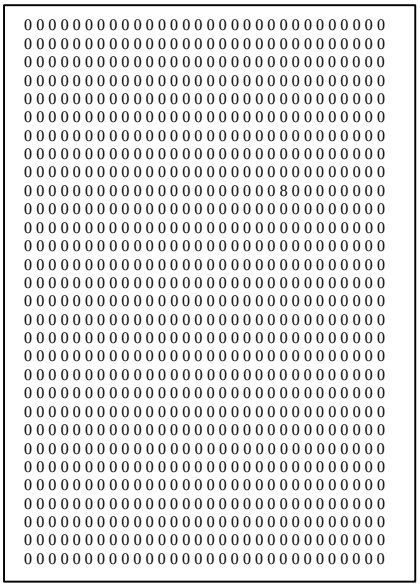
第 7 類的正常行為模式測試資料是用來測試已知的第 6 類式正常行為模式之正常行為模式定義偵測，我們以訓練後已知的網路拓樸來做正常行為資料作分析比對，來衡量訓練後的網路拓樸在偵測已知正常行為模式的效果，研究中發現有 0.842 的偵測準確度。



圖四　類別 7 單位時間 5 秒測試範例在網路拓樸呈現結果

4.3 自我組織映射網路在不正常行為模式之偵測的分析結果

本計畫之自我組織映射網路之入侵偵測模式除了可偵測已知的攻擊行為模式外還要達到可偵測新型未知的攻擊行為模式,所以本計畫加入已知的攻擊行為模式資料外還加入正常使用者行為模式之定義資料,當有資料不屬於已知的攻擊行為模式資料和已知的正常使用者行為模式之定義資料時，表示此資料為新型的未知行為模式資料，分析後的資料叢集範圍如圖五所示。
第 8 類的 synk4 攻擊程式是用來測試未知的新型攻擊行為模式偵測,我們以訓練後已知的網路拓樸來做未知攻擊資料作分析比對,來衡量訓練後的網路拓樸在偵測未知的攻擊行為模式的效果，測驗結果顯示第 8 類的 synk4 攻擊未落入任何已知的叢集範圍中。



圖五　類別 8 單位時間 5 秒測試範例在網路拓樸呈現結果

4.4 未知行為模式偵測的分析結果

在本計畫中根據模糊專家系統的入侵偵測模式,如果使用者的行為為未知的行為模式時會將此封包資料重新送入系統中做訓練與學習，並對模糊專家系統中的模糊規則庫與隸屬函數作調整，以期日後可以偵測出此未知的行為模式。

根據前一節，我們將 synk4 攻擊程式定義為
擊的訓練範例送入倒傳遞網路中學習，增加一條
後重新將其五十筆的待推案例輸入系統中,觀察
觸發的模糊規則為何種行為模式，然後根據收
一、倒傳遞網路重新訓練與模糊專家系統調整

待推案例	RESULT 值	推論結果	待推案例	RESULT 值	推論結果
1	0.6415	synk4 attack	26	0.6415	synk4 attack
2	0.6415	synk4 attack	27	0.6415	synk4 attack
3	0.6415	synk4 attack	28	0.6415	synk4 attack
4	0.781333	normal	29	0.6415	synk4 attack
5	0.641225	synk4 attack	30	0.6415	synk4 attack
6	0.6415	synk4 attack	31	0.6415	synk4 attack
7	0.6415	synk4 attack	32	0.6415	synk4 attack
8	0.6415	synk4 attack	33	0.6415	synk4 attack
9	0.6415	synk4 attack	34	0.6415	synk4 attack
10	0.6415	synk4 attack	35	0.6415	synk4 attack
11	0.6415	synk4 attack	36	0.6415	synk4 attack
12	0.6415	synk4 attack	37	0.6415	synk4 attack
13	0.6415	synk4 attack	38	0.6415	synk4 attack
14	0.6415	synk4 attack	39	0.6415	synk4 attack
15	0.6415	synk4 attack	40	0.6415	synk4 attack
16	0.6415	synk4 attack	41	0.6415	synk4 attack
17	0.6415	synk4 attack	42	0.781333	normal
18	0.6415	synk4 attack	43	0.6415	synk4 attack
19	0.6415	synk4 attack	44	0.6415	synk4 attack
20	0.6415	synk4 attack	45	0.6415	synk4 attack
21	0.6415	synk4 attack	46	0.6415	synk4 attack
22	0.6415	synk4 attack	47	0.6415	synk4 attack
23	0.6415	synk4 attack	48	0.6415	synk4 attack
24	0.6415	synk4 attack	49	0.6415	synk4 attack
25	0.6415	synk4 attack	50	0.6415	synk4 attack

我們將 synk4 攻擊程式的 254 筆訓練範例重新送入倒傳遞網路學習，對倒傳遞網路各項參數設定同表 3-11，結果經過 955 個學習循環後達到收斂的結果，也就是 RMS<=0.05 時。

此時我們再對模糊規則庫新增一條模糊規則如下：

IF I Value IS VERY Low AND IP Value IS VERY Low AND T Value IS VERY High AND U Value IS VERY Low
THEN RESULT is SYNK4 ATTACK

所定義的正常行為和 synk4 攻擊為 TCP 協定，所以將其隸屬函數區間設定為相鄰，將隸屬函數圖最佳化調整。如此一來，入侵偵測模糊專家系統便可偵測出此未知的攻擊行為模式。

二、未知行為模式偵測的分析結果

根據上節對未知的攻擊行為模式重新輸入倒傳遞網路訓練與模糊專家系統調整，本節將對其偵測的效果做驗證。本計畫中定義 synk4 攻擊程式為未知新型攻擊行為模式，重新將其五十筆的待推案例輸入系統中，觀察待推案例在隸屬函數圖中的數值經過模糊推論所觸發的模糊規則為何種行為模式，然後根據收斂表[14]分析其準確度，研究中發現有 0.96 的偵測準確度。

針對此未知行為模式待推案例重新輸入系統推論如圖六所示。而此未知行為模式偵測根據收斂表分析，結果如表四所示。

圖六 未知行為模式待推案例推論結果

表四 未知行為模式偵測的收斂表分析

	系統推論為是	系統推論為否	
實際行為模式為是	48	2	50

五、計畫成果自評

本計畫將入侵行為模式的資料與正常使用者的行為資料合併交由自我組織映射網路分析。網路輸出結果會根據入侵行為模式特徵與正常使用者行為模式特徵做自我叢集的作用，每一個不同類型的攻擊模式與正常使用者行為模式將會分類，當一筆新的輸入資料交由自我組織映射網路分析後，分析其輸出結果是坐落在哪一個叢集範圍內，若是攻擊行為模式的叢集範圍內則是表示入侵行為發生，相對的若坐落在正常行為模式的叢集範圍內則表示為合法的使用者；當其輸出結果不屬於任何一個已知的叢集範圍時，表示此筆輸入資料為未知的行為模式，可能為新型的攻擊行為模式或是正常的行為模式。如此一來不但可以偵測出已知的攻擊模式也可以偵測出新型的攻擊行為模式，而同時達到不正常行為偵測與入侵行為定義偵測的效果，並使用模糊專家系統與倒傳遞網路架構對未知的行為模式重新訓練調整之後做出正確判斷。整理後的偵測結果如表五所示，其結果都有不錯的表現。

表五 單位時間 5 秒下各種入侵偵測模式的偵測準確度

	入侵行為模式	正常行為模式	不正常行為模式	未知行為模式
單位時間 5 秒	0.865	0.842	1	0.96

本計畫經由實驗結果證明了自我組織映射網路可將不正常行為偵測法與入侵定義偵測法結合，達成相互彌補的作用，只要輸入變數的設計可以表現出偵測目標特徵，就可以有很好的偵測效果，所以本計畫的入侵偵測模式可運用在各種入侵攻擊模式上。

六、參考文獻

[1] 林泰維, “利用環境因素考量考量入侵偵測系統分析工具的選取方法”，私立中原大學資訊工程研究所,碩士論文,1990.

[2] 周正宏, 類神經網路-理論與實務, 台北:松崗書局, pp.3-17,1996.

[3] 楊子翔、蔡錫鈞, “Network DoS/DDoS 攻擊及預防方法之研究”，台灣區網際網路研討會, pp.92-101,2000.

[4] 張智晴、林盈達，“網路的攻擊與防護機制”,台灣區網際網路研討會，pp.102-109,2000.

[5] H. Debar, M. Becker, and D. Siboni,“A Neural Network Component for an Intrusion Detection”, Proceedings of the IEEE Computer Society Symposium Detection System , pp.240-250,May 1992.

[6] J. E. Dickerson and J. A. Dickerson,“Fuzzy Network Profiling for Intrusion Detection”,IEEEnetwork, pp.301-306,2000.

[7] J. M. Bonifacio Jr, A. M. Cansian,A. C. P. L. F. de Carvalho “ Neural Network Applied in

Intrusion Detection", IEEE Internation Joint Conference on Neural Networks,vol. 1, pp.205-210,1998.

[8] L. Girardin , "An eye on networkintruder- administrator shootout " , Proceedings of the Workshop on Intrusion Detection an Network Monitoring ,1999.

[9] R. G. Bace, Intrusion Detection. Indianapolis, IN: Macmillian Technical publishing,2000.

[10] R. P. Lippmann and R. K. Cunningham, "Improving intrusion detection performance using keyword selection and neural networks", Computer Network 34 , pp.597-603,2000.

[11] S. Northcutt and J. Novak, Network Intrusion Detection: An Analyst's Handbook. 2nd Edition, Indianapolis IN:New Riders Publishing, 2001.

[12] T. F. Lunt, "Panel:Foundations for Intrusion Detection?", IEEE network, pp104-106, 2000.

[13] Teuvo Kohonen , "Self-organizing maps", Berlin, Heidelberg , New-York：Springer,1995.

[14] Lewis, D. D. (1995). Evaluation and optimizing autonomous text classification systems. *SIGIR*, 246-256.

成果發表說明

本計畫之部分結果將發表於第 37 屆 International IEEE Carnahan Conference:

Dwen-Ren Tsai, Wen-Pin Tai, Chi-Feng Chang, " *A hybrid intelligent instrusion detection system to recognize novel attacks*," The 37th International IEEE Carnahan Conference, Taipei, Taiwan, October 14-16, 2003.