以 MSN 即時通訊朋友關係為基礎校園網路安全監控系統之設計與實作

洪丞緯 歐育智 張凱翔 蔡志汶 蘇暉凱*
南華大學資訊工程學系
hksu@mail.nhu.edu.tw*

摘要

網路行為是使用者所觸發，隨著使用者更換上網地點與更換上網電腦，往往降低傳統網路安全機制之準確性，無法即時提供網路安全保護。因此，本論文在校園網路環境，提出以 MSN 朋友關係網為基礎之校園網路安全監測與控制系統。本論文提出的網路安全監控工作可分為：1. MSN 封包資料監測、2. MSN 協定分析、3. MSN 朋友關係網分析、4. 防火牆決策與控制。主要概念是事先分析 MSN 使用者行為，根據 MSN 使用者交友關係、聊天行為，以及 IDS (Snort) 警告事件之輔助資訊，進行防火牆允許控制動態規則之決策。因此，本系統可隨使用者更換上網地點或更換上網電腦，動態調整防火牆允許控制規則，協助網路安全維護與管理等重要工作。[1]

關鍵字：MSN 即時通訊、網路安全、網路監測、防火牆

Abstract

Network behavior is driven by network users. With the ability of changing location and changing terminal device to access Internet, the accuracy of network security mechanism would be decreased, and the network security and protection could not be provided on real time. Thus, this paper proposes a MSN friendship-network-based campus network security monitor and control system in a campus network environment. The proposed tasks of network security monitor and control, including 1) MSN packet capturing, 2) MSN protocol analyzing, 3) MSN-friendship network analyzing, and 4) firewall policy decision and control. The key ideal is that analyzing MSN users' behavior in advance. According to the MSN friendship, the chat behavior and the external warning events from IDS (Snort), the dynamic firewall rules are decided. Therefore, once users change location or terminal device to access Internet, this system can adapt the firewall rules dynamically. This contribution can support the important tasks about network security maintenance and management.

Keyword: MSN Instance Messenger, Network Security, Network Monitor, Firewall

1. 前言

隨著網際網路的普及和技術的進步，傳輸速度與品質也逐年提昇，直接加快網路攻擊與病毒散佈之速度，縮短駭客搜尋與攻擊的時間；一些不合法的小動作，都可能在一瞬間癱瘓整個網路服務。因此，網路安全監測與控制是網路管理中一項非常重要的工作，如何在高速分封交換的環境中，提供精確且高效益的網路安全監控服務是一項具挑戰性的技術。

另一方面，隨著高速寬頻的普及，快速增加人與人通訊的寬度與廣度，MSN 即時通訊軟體即是一典型例子。MSN 用戶數近幾年快速成長，於 2008 年已超過 225 萬位使用者[1]。然而，相對於傳統網際網路，目前使用者上網地點常更換，並且常使用不同電腦上網，因此，傳統網路安全技術透過一般防火牆 (Firewall)、IDS (Intrusion-Detection System；入侵偵測系統)、IPS (Intrusion-Prevention System；入侵防禦系統) 已無法滿足當前以網路使用者為導向之網路安全需求。

目前網路安全的管制皆架構在防火牆之基礎上，一般防火牆防衛架構皆屬於事先定義防衛規則 (Proactive Defense)，當網路開始運作時，及以該事先定義好的防火牆規則管制網路。而事後防衛規則 (Reactive Defense) 是架構在 IDS 或 IPS 的基礎下，當發現入侵行為後，適時給予反應及管制。但無論是 Proactive Defense 或 Reactive Defense，最終還是必須依據網路封包特徵給予控制；換句話說，也就是阻擋某個 IP Address、阻擋某台電腦之資料流、阻擋某種應用服務之封包。但上述解決方案皆只是處理暫態的表象，在保護成效與理想上仍有段差距。

本論文提出以 MSN 朋友關係網為基礎之校園網路安全監測與控制系統，以校園網管人員的觀點切入，在校園網路環境中，事先收集與分析 MSN 通訊資料，定義與建構 MSN 朋友關係網，以提供防火牆允許控制策略制定之重要參考資料；除此之外，根據透過 MSN 使用者登入資料監測、MSN 朋友關係強度與 Snort[2]外部系統警告事件之數據，本系統可以決定出火牆允許控制之動態規則，保護使用者遭受各種具有敵意性的攻擊。最後，本系統結合先進 Web Application 技術與 Google Maps

[1]本研究由國科會贊助，計畫編號 NSC-96-2221-E-343-001。

技術，整合地理資訊與網路安全資訊，提供一友善網路安全管理介面，讓系統管理者與一般使用者可以快速、方便地瞭解網路安全狀況。

2. 背景

2.1 Ontology Analysis

本體論 (Ontology) 是人工智慧中一種知識表現方法，是一種形式化共享概念的明確表述。本體論的使用領域除了人工智慧、詞彙語意 Web 應用技術、軟體工程、生物資訊、圖書科學與資訊結構 (Information Architecture)，作為該領域呈現全部或部份知識的一種方法[3]。

Ontology 的結構包含以下幾個元素：

- Individuals (Instances)：是 Ontology 的基礎元素，可能是有形的物件，例如：公車、汽車，也有可能是無形的個體，如：數字、文字。
- Classes (Concepts)：是一種抽象的群組或類別，例如：交通工具 Class 包含公車與汽車 Individuals。
- Attributes：在 Ontology 下的物件，皆可以定義 Attributes (屬性) 來描述。
- Relationships：用來描述物件間的關係。

由於人與人之間的關係強度，跟知識之間的結構相似，故本研究將參考 Ontology 的結構概念，定義與建立 MSN 朋友關係網，本論文標示的 Relationships 即朋友關係，除了明確標示在好友名單的朋友關係外，並推算出其他使用者間朋友關係強度，提供防火牆允許控制策略制定之重要參考數據。

2.2 Google Maps API

Google Maps 為一種網路電子地圖，它可以顯示局部的地理資訊與衛星地圖，顯示的範圍涵蓋至全世界。

Google Maps API[4]，提供程式設計者可以方便地將地理資訊服務整合到應用程式中。目前 Google Maps API 提供三種版本，分別是 JavaScript Version、Flash Version 與 Earth Version。就差異性而言，JavaScript Version 為最早的版本，功能最齊全；Flash Version 的優點則是所佔用的 CPU 資源最少；而 Earth Version 的特色在於它的 3D 化介面。

本論文將採用 Google Maps API-JavaScript Version，整合地理資訊與網路安全資訊，在校園網路安全管理介面上，可以清楚瞭解校園網路設備運作狀況、網路拓樸與地理資訊，並且呈現每位 MSN 使用者上線的地理位置，讓網路管理人員可以清楚地瞭解網路安全狀況，增加網路安全危機處理之效益。

3. 系統架構

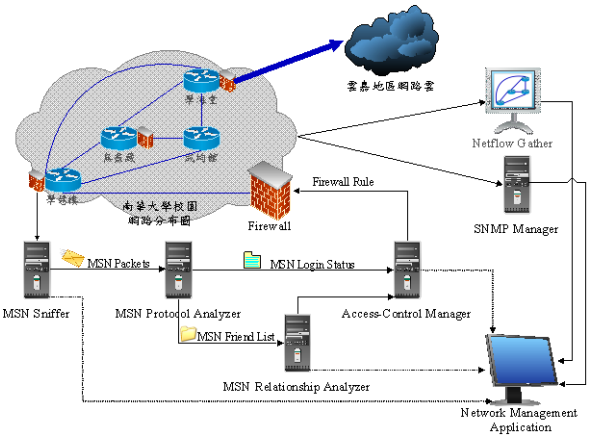


圖 1 系統環境架構圖

本系統以南華大學校園網路為實驗環境，如圖 1 所示，系統主要元件描述如下：

1. MSN Sniffer：負責擷取網路上 MSN 相關的封包，MSN Sniffer 可以佈署在校園網路重要連線節點上，以被動方式監測，在不影響現有網路運作的情況下，進行 MSN 封包擷取。
2. MSN Protocol Analyzer：負責解析 MSN Protocol 內容，收集 MSN 使用者之 MSN Friend List、MSN Login Status 與聊天記錄。
3. MSN Relationship Analyzer：根據所收集的 MSN Friend List、MSN Login Status 與聊天記錄，負責分析 MSN 朋友關係網，除了明確標示在 MSN Friend List 的關係外，並推算出朋友的朋友關係強度，本系統將推算出所有間接之朋友關係強度；隨著朋友關係網的大小，建議可以推算三到五級間接關係，以降低複雜度。
4. Access-Control Manager：將參考所分析之朋友關係網、外部 Snort 系統所產生之警告事件與目前 MSN 使用者登入狀態，動態制定防火牆允許控制之規則。Access-Control 將在 MSN 使用者登入與登出時，更動該使用者相關之防火牆規則；除此之外，如果 Snort 有重要攻擊警告事件，也將更動相關防火牆規則，細部條件請參考 4.3 節。
5. Netflow Gather 與 SNMP Manager：負責蒐集 CISCO Netflow[5]資訊與透過 SNMP (Simple Network Management Protocol)[6]蒐集網路設備與連線狀況，提供網路安全輔助資訊。
6. Network Management Application：提供一友善網路安全管理介面，該管理軟體整合 Google Maps 地理資訊、網路拓樸與網路安全資訊，包含 MSN 監測資料、已分析之 MSN 朋友關係網、防火牆允許控制之動態規則…等資訊，讓網路管理人員可以快速且明確地瞭解網路安全運作狀況。

本系統除了採用現有 Netflow Gather、SNMP

Manager 與 Snort 相關軟體外，其餘軟體元件皆自行開發，包含 MSN Sniffer、MSN Analyzer、MSN Relationship Analyzer、Access-Control Manager 與 Network Management Application。下一章節，我們將針對所發展之軟體元件進行詳細介紹與說明。

4. 元件設計

4.1 MSN Sniffer and Analyzer

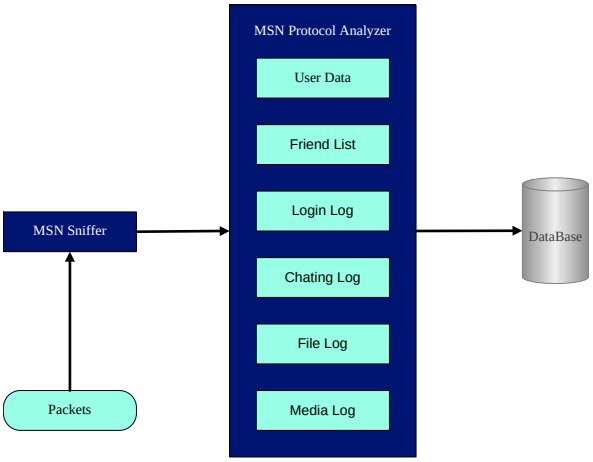


圖 2 MSN Sniffer 功能方塊圖

本元件之功能方塊圖如圖 2 所示，透過 MSN Sniffer 元件抓取網路中所有 MSN 封包，並交由 MSN Protocol Analyzer 分析[7]，分析完畢後立即存入資料庫供其他元件使用。

其中 MSN Protocol Analyzer 分析資訊如下：

- 使用者資訊：使用者帳號、使用者暱稱。
- 使用者好友資訊：好友帳號、類型 (是否為封鎖對象)、好友狀態 (上線、離線、忙碌等等)。
- 使用者登入資訊：使用者上線時間、使用者在線時間、IP 位址。
- 交談訊息記錄：使用者與好友之交談記錄。
- 檔案傳遞記錄：使用者與好友之檔案傳遞記錄。
- 多媒體訊息記錄：使用者與好友之多媒體訊息記錄 （語音、視訊等等…）。

4.2 MSN Relationship Analyzer

本元件參考 Ontology 之觀念，依據 MSN Sniffer 元件所擷取出來之好友名單及封鎖清單，建構 Relationship Network，並推算出所有關係強度。

首先，本元件定義系統參數如下：外部輸入參數 (表 1)、內部計算與輸出參數 (表 2)，以及系統參數 (表 3)。

朋友關係計算式說明如下：

- 朋友關係強度 $\bar{r}_{ij}$ （計算式 (1)）：關係強度之權重指數 α ，取好友名單關係強度 $(r`_{ij})$ 與聊天頻率 (c_{ij}) 之加權平均，推算出最後關係強度 i 與 j 的朋友關係數值。若 j 不在 i 好友名單中 $(r_{ij} = 0)$，則需計算此關係強度；反之，從量測資料已得到關係強度，則直接給予關係強度 $(\bar{r}_{ij} = r_{ij})$ 值。
- 推測之好友名單關係強度 $r`_{ij}$ (計算式 (2))，以下分兩種情況說明：
  - 第一種：若 R_{ij} 中 $r_{xy} \neq -1,\ \forall(x,y) \in R_{ij}$ 成立時，表示最短連鎖關係連結中，所有連鎖關係皆不為負面封鎖關係；因此，此間接關係可推測。在最短連鎖關係連結中，將所有關係強度，依 β 指數 d_{ij} 次方遞減相加及平均，最後求得 $r`_{ij}$；關係連結越近，加權越重，關係連結越遠，加權越輕。
  - 第二種：反之若 R_{ij} 中 $r_{xy} = -1,\ \exists(x,y) \in R_{ij}$ 存在時，表示挑選最短關係連接中存在著封鎖關係，此推測結果不明確；因此，本元件將 $r`_{ij}$ 直接設定為 0。例如：A 與 B 為親密關係，B 與 C 的關係為不友善，最後 A 與 C 的關係並不一定是親密，也不一定是不友善；因此，在這種情況下，我們歸類此關係為不明確關係。
- 登入聊天頻率 c_{ij} (計算式 (3))：將使用者登入次數與登入並聊天次數相除，以計算聊天頻率 c_{ij} 。

$$\begin{cases} \bar{r}_{ij} = \alpha\, r`_{ij} + (1-\alpha)c_{ij}\,, \text{if } r_{ij} = 0; \\ \bar{r}_{ij} = \alpha\, r_{ij} + (1-\alpha)c_{ij}\,, \text{otherwise.} \end{cases} \tag{1}$$

$$\begin{cases} r`_{ij} = \dfrac{\sum_{(x,y)\in R_{ij}} \beta^{d_{iy}} r_{xy}}{d_{ij}} & , \text{if } r_{xy} \neq -1, \forall(x,y) \in R_{ij}; \\ r`_{ij} = 0 & , \text{otherwise.} \end{cases} \tag{2}$$

$$c_{ij} = \frac{t_{ij}}{l_i} \tag{3}$$

表 1 輸入參數表

參數	定義說明
U	MSN 使用者集合。
R_{ij}	表示 i 到 j 最短好友關係距離之使用者連鎖關係連結集合。$i \in U,\ j \in U$ and $i \neq j$。例如：i 到 j 最短朋友關係距離是經過 k，因此 $R_{ij} = \{(i,k),(k,j)\}$。
r_{ij}	表示從 MSN Sniffer 中擷取到之朋友關係強度。如果 j 在 i 的朋友名單中，表示 $r_{ij} = 1$；如果 j 在 i 的封鎖清單中，表示 $r_{ij} = -1$。 $i \in U,\ j \in U$ and $i \neq j$。
l_i	表示 i 在近 n 天內登入之次數。
t_{ij}	表示 i 在近 n 天內，曾與 j 聊天之登入次數。

表 2 內部計算與輸出參數表

參數	定義說明
$\bar{r}_{ij}$	表示最後加權所推算之朋友關係強度，亦為最後欲求得之參數。
$r`_{ij}$	表示是透過朋友名單與封鎖清單所推測出來的好友名單關係強度。 $-1 \le r`_{ij} \le 1,\ i \in U,\ j \in U \text{ and } i \ne j$
d_{ij}	表示 i 對 j 的關係距離。如果 j 是 i 朋友的朋友，則 $d_{ij} = 2$。
c_{ij}	表示 i 對 j 聊天的頻率，當 i 每次登入 MSN 皆曾與 j 聊天，其 $c_{ij} = 1$；反之，若皆未曾與 j 聊過天，其 $c_{ij} = 0$。$i \in U,\ j \in U \text{ and } i \ne j$

表 3 系統參數表

參數	定義說明
α	表示朋友名單與聊天頻率所推算出朋友關係強度之權重指數。 $0 \le \alpha \le 1$
β	表示朋友關係強度，隨關係距離增加之下降指數。$0 \le \beta \le 1$

本元件將關係強度分為三個等級，分別定義如下：

- 親密關係：當 $\bar{r}_{ij} \ge 0.4$，雙方傳輸為可靠性關係。
- 不明確關係：當 $0 \le \bar{r}_{ij} < 0.4$，雙方關係不明確，因此必須參考外部系統 (Snort) 之警告訊息，判斷是否為攻擊行為，並決策是否阻擋該關係之所有封包。
- 不友善關係：為 $\bar{r}_{ij} < 0$，雙方關係為不友善關係，因此必須阻擋兩者間相關封包。

4.3 Access-Control Manager

如圖 3，Access-Control Manager 輸入目前使用者登入狀態、已分析之朋友關係強度，以及 Snort 警告事件的外部資訊，最後由內部 Traffic Control Decision 處理，判斷 MSN 登入者與其他使用者是否可能違反網路安全之行為，並產生出相對應之動態防火牆規則。

如圖 4，當 MSN 使用者登入資訊輸入至 Traffic Control Decision 中，根據朋友關係圖查詢 MSN 登入者與其朋友關係強度。當強度大於等於 0.4 時，將其所傳輸的封包建立至通行規則之中；當強度大於等於 0 且小於 0.4 時，則參考 Snort 警告事件，分析該使用者是否具有攻擊行為，如結果為是，則將其名稱建立至阻擋規則之中，如結果為否，則將其名稱建立至通行規則之中；當關係強度小於 0 時，則其所傳輸的資訊可能為攻擊行為，並將其建立至阻擋規則之中。接著，將通行規則與阻擋規則整合，並比對所有動態規則之矛盾問題與重複問題，最後輸出動態允許控制規則。

由於網路並不是每個使用者都會使用 MSN，因此本系統在防火牆管理策略上採用封鎖清單管制，最後所有動態允許控制規則都會轉換成阻擋規則。如果對網路安全要求更嚴格，則可考慮使用封鎖清單管制。

最後，透過動態允許規則之產生，在彙整預先設定之防火牆靜態規則，最後將彙整過之防火牆規則實施到防火牆上，當不友善之攻擊事件發生時，便可立即產生防禦的功效。

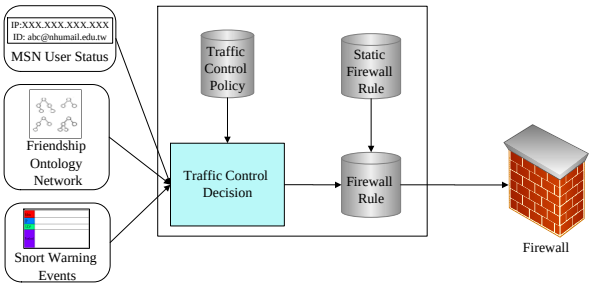


圖 3 Access-Control Manager 示意圖

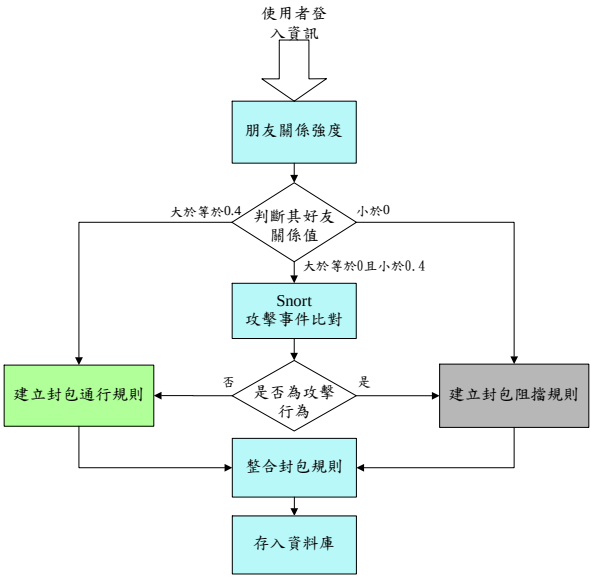


圖 4 Traffic Decision 流程圖

4.4 Network Management Application

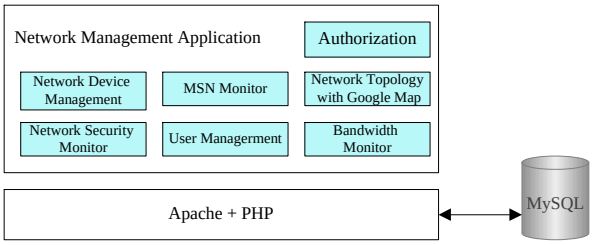


圖 5 網頁功能元件圖

本元件以 PHP 程式語言發展 Web 網路管理應用程式，以 Apache HTTPD 提供穩定之 Web 服務，後端搭配 MySQL 資料庫系統儲存與管理資料。如圖 5，本論文自行開發會員驗證、網路設備

管理、MSN 監視、網路地域拓樸圖、網路安全監視、使用者管理與流量監視等七大功能，提供完整網路安全管理系統功能。

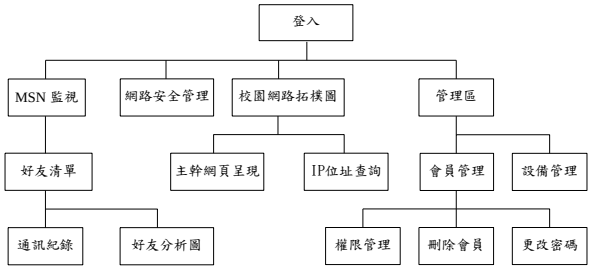


圖 6 網頁介面架構圖

本系統網頁介面架構圖如圖 6，並提供以下功能：.

- MSN 監視：顯示出在校園內登入 MSN 帳號使用者的資料，包含個人帳號、登入時間、IP、朋友交流次數、朋友清單、對話內容。
- 校園網路拓樸圖：利用 IP 位址及搭配 Google Maps 顯示目前 MSN 使用者的登入所在位置。
- 好友分析圖：利用上述資料建立出一份交友狀況拓樸圖，顯示某一 MSN 使用者與其他人的朋友關係。
- 網路安全管理區：使用者登入後可以利用網路管理知道校園網路中 router 與 switch 的運作與流量狀況。
- 會員管理：本網頁以會員制度作管理，以方便權限上的設定，以及新增、更改、與刪除會員資料。
- 設備管理：建構於管理區部分，可連進網路設備之中，並修改內部設定。

5. 案例說明

本章節，為簡化說明之複雜度精簡實際運作資料，以一案例說明本系統之運作流程與結果。

5.1 MSN 朋友關係網事前分析

首先假設，MSN Sniffer 元件擷取之資料如表 4，分別為使用者、好友名單，以及封鎖清單，例如 U1 的好友名單有 U3，封鎖清單則是在 U5。在經過擷取後我們將表 4 的資料交由 MSN Relationship Analyzer 元件分析。在此，我們假設不考慮聊天頻率參數，因此系統參數 α 設為 1，而 β 設為 0.7，再將所有已知關係強度帶入計算式 (1)，即可求得朋友關係強度，為長期觀察所求得之朋友關係網，如圖 7 所示，圖中紅色字為 MSN Sniffer 元件所提供之 r_{ij} ，綠色字為推算得到之 $\bar{r}_{ij}$ 。

表 4 MSN 使用者資訊

使用者	好友名單	封鎖清單
U1 (u4009080@nhumail.edu.tw)	U3	U5
U2 (u4009065@nhumail.edu.tw)	U4、U5	U3
U3 (u4009060@nhumail.edu.tw)	U1、U4	U2
U4 (u4009061@nhumail.edu.tw)	U2、U3	
U5 (u4009072@nhumail.edu.tw)	U1、U2	

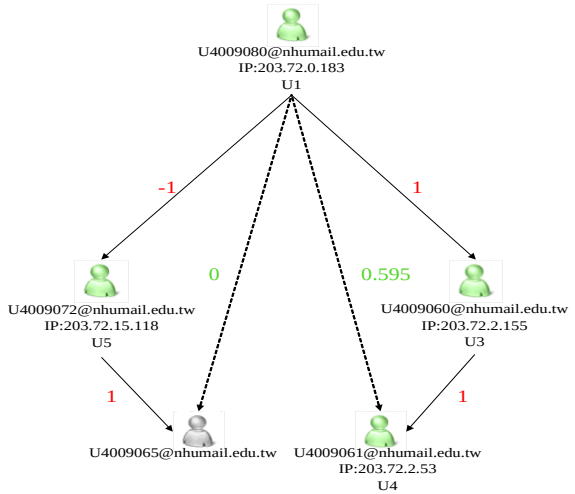


圖 7 MSN 朋友關係網

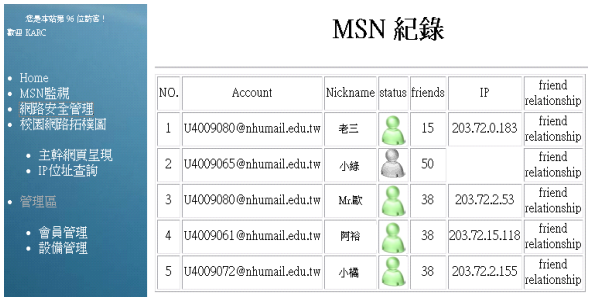
5.2 防火牆允許控制動態規則之產生

表 5 防火牆行為決策表

編號	來源位置	目的位置	來源埠/目的埠	協定	動作
1	203.72.2.115	203.72.0.183	any/any	TCP/UDP	accept
2	203.72.15.118	203.72.0.183	any/any	TCP/UDP	deny
3	203.72.2.53	203.72.0.183	any/any	TCP/UDP	accept

承 5.1，假設當 U1 從 IP Address 203.72.0.183 登入 MSN，系統會根據已分析的朋友關係網與 MSN 使用者上線資訊，產生相關的防火牆允許控制之規則。因為本系統目前假設 Snort 沒有產生任何的警告事件，所以直接以朋友關係強度當作阻擋資訊之判斷依據。當 U3 從 IP Address 203.72.2.115 傳輸資訊給 U1 時，因為 U3 在 U1 的好友名單之中，所以強度為 1 (親密關係)，並將其 IP 設定為允許傳輸；當 U5 從 IP Address 203.72.15.118 傳輸資訊給 U1 時，因為 U5 在 U1 的封鎖清單之中，所以強度為 -1 (不友善關係)，並將其 IP 設定為拒絕傳輸；當 U4 從 IP Address 203.72.2.53 傳輸資訊給 U1 時，因為 U4 不存在 U1 的好友名單之中，經過 MSN Relationship Analyzer 的強度分析公式分析過後得到關係強度為 0.595 (不明確關係)，所以便將 U4 之 IP 設定為允許傳輸。

5.3 網路管理介面展示



NO.	Account	Nickname	status	friends	IP	friend relationship
1	U4009080@nhumail.edu.tw	老三		15	203.72.0.183	friend relationship
2	U4009065@nhumail.edu.tw	小綠		50		friend relationship
3	U4009080@nhumail.edu.tw	Mr.歐		38	203.72.2.53	friend relationship
4	U4009061@nhumail.edu.tw	阿裕		38	203.72.15.118	friend relationship
5	U4009072@nhumail.edu.tw	小橘		38	203.72.2.155	friend relationship

圖 8 MSN 使用者狀態列表圖

如圖 6，在使用者登入網頁後，可依使用者選擇，顯示 MSN 監視狀況，所顯示的資料為在校園網路內登入的 MSN 帳號，如圖 8，包含：帳號、別稱、狀態、朋友人數及 IP 位址，其中編號 2 的帳號目前並未在校園網路中上線，所以其顯示的 IP 位址為空白，而在點選 friend relationship 選項，則可以顯示每筆帳號的 MSN 朋友關係網，如圖 9，記錄著 U4009080@nhumail.edu.tw 帳號使用者的交友情況，其中灰色代表目前並未上線，而綠色則代表上線，其中關係強度接近 1 的代表好友；而接近 -1 則代表關係差。

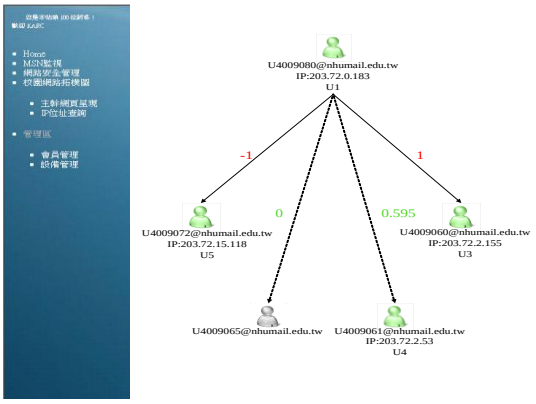


圖 9 MSN 朋友關係網之呈現結果

圖 10 網路地域拓樸圖

如圖 10，利用以上資料搭配 Google Maps 追蹤和顯示目前上線使用者的所在位置，顯示目前上線者所在位置及 IP Address。除此之外，各大樓上的旗標，記錄著各大樓的名稱與流量，利用 Google Maps 的功能顯示出主幹網路流量與各大樓之間的流量，其中紅色線代表各大樓的流量，在匯集到主大樓之後，經由主幹道流出校園網路，並用綠色線表示。點選連線後可呈現該連線流量圖；點選設備旗標可呈現該設備運作狀態。包含防火牆的運作狀態。

6. 結論

本論文突破傳統以阻擋特定 IP Address 的方式，以人為出發點，設計 MSN 朋友關係強度分析機制，作為阻擋攻擊行為之重要參考，以達到即時安全防護。因此，無論使用者如何更換地點或更換使用電腦，我們都能根據所擷取到的登入者資訊，產生的動態防火牆規則來鎖定不友善使用者之 IP Address。除此之外，本系統結合先進 Web Application 技術與 Google Maps 技術，整合地理資訊與網路安全資訊，讓系統管理者與一般使用者可以快速、方便地瞭解網路安全狀況。本系統以校園網路為測試環境，但礙於個人隱私權，以及龐大且複雜之 MSN 朋友關係資訊，都將造成實際運作之困難。因此，網路安全相關法律規範、如何降低關係網分析複雜度與如何提供更精準之關係推測，都將是未來可以努力的方向。

參考文獻

[1] MSN - wikipedia, http://en.wikipedia.org/wiki/MSN.

[2] Snort - the de facto standard for intrusion detection/prevention, http://www.snort.org/.

[3] N. F. Noy and M. A. Musen, “Ontology Versioning in an Ontology Management Framework,” IEEE Intelligent Systems, vol. 19, no. 4, pp. 6-13, July 2004.

[4] Google Maps API, http://code.google.com/apis/maps.

[5] Cisco IOS NetFlow, http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[6] D. Harrington, R. Presuhn and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks," STD 62, RFC 3411, December 2002.

[7] MSN Messenger Protocol, http://www.hypothetic.org/docs/msn/.