實作一個 SIP 垃圾電話偵測系統

游坤明 陳宗欣
中華大學資訊工程系
{yu ; ericcute}@pdlab.csie.chu.edu.tw

摘要

近年來網際網路的應用可以說是日新月異，在許多的技術與應用不斷的推陳出新下，逐漸的成為人與人之間重要的溝通管道，而網路電話（VoIP）便是其中的一種。隨著網路電話的逐漸普及，網路電話的安全性將會成為未來一個重要的議題。其中，垃圾網路電話（SPIT，Spam call）的防堵就是一門重要的學問，尤其是當網路電話像電子郵件一樣盛行時，使用者能夠正確地識別並且進行防堵大量的非法網路電話。雖然，目前網路電話在現今社會上並沒有出現太過嚴重的垃圾網路電話，但有效的防範與識別垃圾網路電話卻是刻不容緩的。因此本論文提出了一個有效的垃圾網路電話偵測系統架構，這個架構可以讓使用者針對他的朋友設定一個信任值，並且透過人與人之間的名譽關係概念，以廣度優先的演算法逐一搜索與計算信任等級，並且與一個門檻值作比較，進而辨別來源者是否為一個合法的呼叫者，以達到辨識垃圾網路電話的功能。

關鍵詞：網路電話、垃圾網路電話、名譽關係

1. 前言

因應網際網路的蓬勃發展，網路的應用也隨之變得多樣化，而 IP（Internet Protocol）電信產業的問世與快速的發展下，網路電話就由此應運而生，而 VoIP 的特點在於利用現有開放性的網際網路，傳送語音至全球各地，讓使用者可以不需要透過傳統的公眾電話網路（PSTN；Public Service Telephone Network）的服務，即可無遠弗屆地透過網際網路進行互動式語音交談，並且 VoIP 有逐漸取代傳統電話的趨勢。初期的網路電話多以軟體的形式呈現，但僅僅限制在 PC to PC 間的通話，隨著寬頻的普及與相關網路技術的演進，網路電話也由單純的 PC to PC，發展出 IP to PSTN、PSTN to IP、PSTN to PSTN 以及 IP to IP 等各種形式，而他們之間的共通點，就是以 IP 網路為傳輸媒介。既然是在 IP 網路上運行，甚至是在網際網路上傳遞，那麼與網路安全之間的關連性應該是密不可分，正因如此，相對的也帶來了網路電話的安全性議題。

SPIT（Spam for Internet Telephony）—「垃圾網路電話」，也有人稱之為 Spam Call，SPIT 的議題是在 InBox IT 2005 電子郵件會議中首度被提出的，因為 SPIT 的威脅比電子郵件的垃圾嚴重許多，使得 IP 通訊匯流中的 VoIP 正在促使一種新型態的垃圾郵件產生。

隨著網路通訊科技的興起，VoIP[1,2,9]的確為人類帶來許多積極正面效益，但卻也隱藏著令人擔憂的負面問題—電腦（網路）犯罪與網路安全等重大影響，特別是有心的 VoIP 使用者，藉由預先錄製好的語音資料搭配上 VoIP 的語音服務進行市調、推銷、騷擾，甚至於詐騙等，如此，不但可以降低通話成本與人力資源，更可能運用網路的開放式資源進行自動外撥電話功能，以達到他們所想要的目的。更有些使用者惡意針對企業級的 VoIP 或者是 VoIP 服務的提供者進行所謂的 DoS[7]攻擊，企圖癱瘓 VoIP 的服務以及造成企業的網路出現嚴重的頻寬負荷。

因此我們提出一個有效的網路垃圾電話偵測架構，在這個架構中，除了能夠讓使用者自行設定信任等級與搜尋層級外，還能夠透過信任網路管理進行計算與判別來源者是否為一個合法的呼叫

者，來達到有效偵測垃圾網路電話的功能。

2. 背景與相關研究

2.1 SIP (Session Initiation Protocol)

H.323 在 1999 年以前是最普遍網路電話的標準，但因為它的複雜性高，在許多的技術上受到限制，無法完全符合應用。因此，IEFT（Internet Engineering Task Force）在 1999 年 3 月提出了 SIP（Session Initiation Protocol）[12]新架構，以簡化 H.323 的複雜性，並且在語音傳遞的功能上提供較高的延展性。SIP 採用了明文傳輸（text-based）的方式，具有 Client-Server 架構，且在 IP 封包的處理上，SIP 可以利用 HTTP 既有的封包資訊，而不需要像 H.323 的封包那樣必須保留很多傳輸上的資訊，並且解決了 H.323 在呼叫建立的速度慢與擴充性低的缺點。

SIP 為一個主從式（Client-Server）架構，由用戶端（Client）送出請求（Request），伺服器（Server）接收到請求之後，依情況做出適當的回應（Response）給用戶端。它分別由四種 SIP 元件所組成[8]，用戶端（User Agent）、重新導向伺服器（Redirect Server）、註冊伺服器（Registrar Server）與代理伺服器（Proxy Server）。

2.2 SIP Social Network

信任管理[5]扮演一個有效率與安全相互影響的重要角色，可以讓使用者具體的確認他們認識誰和人與人之間彼此的關係。在這樣的概念基礎下，SIP Social Network[13]就由此而生，在這個架構中提出一種以信譽為基礎的機制，將人與人之間的關係建構成一個彼此有權重（edge-weighted）的圖形來表示，並以 SIP 社群的方式來偵測垃圾網路電話者的攻擊。

在社群網路中，圖形理論經常扮演者重要的角色，而應用圖形的相關屬性來代表使用者的社群網路特徵，其最大的優點是能夠快速及清楚地了解使用者的人際關係資訊。社群網路是一群相互連結的人或者是彼此有相同型態的團體，以這樣的關係建構出一個表示他們之間關係的圖形，而這些有相互關係的一群人都是通訊軟體上的聯絡名單或是好友名單所集合而成，由使用者對於屬於他自己通訊名單上的朋友們可以依照當時情況給予不同的名譽值（Reputation Value），透過這樣的動作，即可以圖形來表示彼此之間的關係，如圖 1 所示。

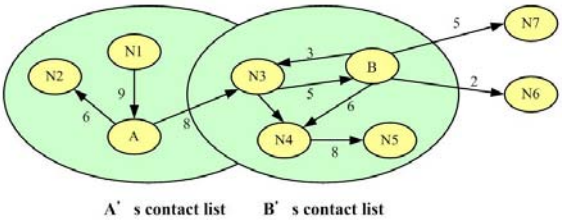

圖 1 SIP 社群網路

2.3 The Small World

根據「史丹佛大學研究中心」的一項調查報告指出，人的一生中所賺的金錢，12.5%來自知識，87.5%則是來自人際關係，這突顯出「人際關係」的重要性。美國心理學家米爾格蘭（Stanley Milgram）更提出了著名的六度分離理論（Six Degrees of Separation），所謂的六度分離理論是指任何兩個沒有任何關係的人，可以經由六個人連結出彼此的某種關係。而康乃爾大學的華茲（Duncan Watts）與史楚蓋茲（Steve Strogatz）對此作了更進一步的研究，進而發表「小世界」網路的集體動力學[4]，提出人際關係、瘟疫、時尚、集體行為等網路科學都與小世界息息相關。所以，對人際網路而言，以六度分離理論為理想，並在人與人彼此信任的基礎上，藉由朋友與朋友之間的關係，擴大人際關係層次的延伸，建立個人虛擬網路社群，如同真實社會的縮影。圖 2 為六度分離理論關係圖。

3. SIP 服務之垃圾電話偵測系統

3.1 系統架構

VoIP 是將語音訊號壓縮成數據資料封包後，在 IP 網路基礎上傳送的語音服務，相同的它也一樣面臨到病毒與駭客的入侵、阻斷攻擊（DoS）、垃圾郵件等等網路安全性的問題，其中，一個逐漸受到重視的議題是，IP 語音系統將受到不法的語音郵件（SPIT）的騷擾。目前針對 SPIT 所做的研究有以黑白名單的方式為基礎，並且加上過濾的方式進行辨別，這樣的方式對於使用者來說，有可能會因為不存在於名單內的人員，而視為一通合法的電話，實則不然。也有其他學者[3,6,10,11]提出點對點回應身份和回應證明來保證回應資訊的健全與隱私，藉此以辨別使用者身份的正確性，但這些的研究都忽略了一點，就是 SPIT 可能出現於一個未知的來源位置，因此，對於這樣的一個問題，本論文提出了一個偵測來源的方式與應用阻擋 SPIT 的封閉式網路架構，在本論文中，以 Social Network[13]搭配六度分隔理論（Six Degrees）為基礎結構，在 SIP 通訊協定上，透過人與人之間的關係，讓系統可以使用 SIP 網路協定建立網路電話並且提供偵測垃圾網路電話的功能。

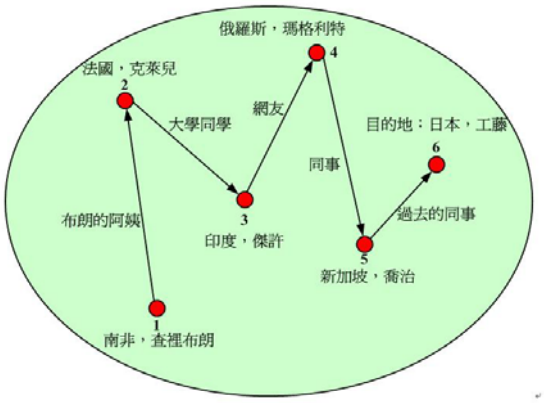

圖 2 六度分離理論關係圖

根據六度分離理論可知，人與人之間只需六個層級，即可讓彼此有某種特定的關係，透過這一特點，系統在偵測 SPIT 時會搜尋至第六層以找出彼此關係的路徑，但因搜尋到第六層所花的時間過長，導致效率降低，無法即時與有效的過濾 SPIT。因此，系統會預設只搜尋三層之間的關係，使用者也可以針對本身的需求進行修改，擴大搜尋層級的範圍。由於 SIP 是一種即時性的服務，因此，有效的防堵 SPIT 也必須是能夠即時的處理，才能符合 SIP 通訊協定的需求。在本研究中，系統架構中的主要元件分為 SPITCatcher（垃圾網路電話捕捉器）和 SPIT Manager（垃圾網路電話管理者）。如圖 3 所示。

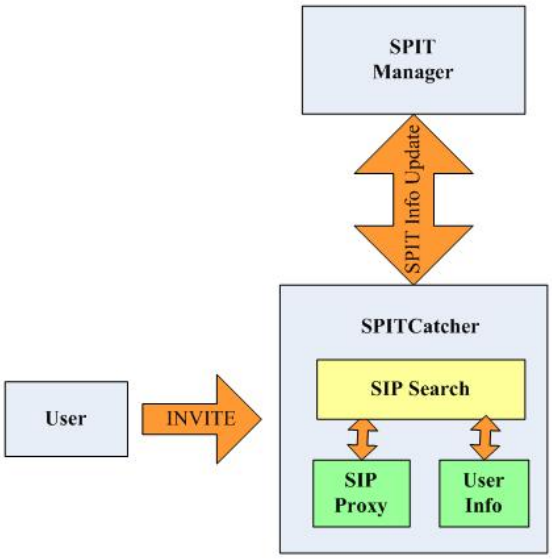

圖 3 SIP 服務之垃圾電話偵測系統架構

3.2 SPITCatcher

SPITCatcher 主要的功能是當 SIP Search 計算完每通電話的信任等級後，將這個值回傳到 SPIT Manager，當有 INVITE 訊息要傳送到 SIP 代理伺服器前，都要經由 SIP Search 進行信任等級運算，並且依照使用者在 SIP Search 所設定的門檻值進行判斷是否為 SPIT。圖 4 為 SPITCatcher 架構，其主要元件由 SIP Search、SIP Proxy 和 User Info 所組成：

- **SIP Search**：主要進行被呼叫者的搜尋與計算相關人員路徑的信任等級。
- **SIP Proxy**：針對 User Agent 所發出的 INVITE 訊息進行處理，並且於予回應以建立連線。
- **User Info**：存放使用者訊息的資料庫，其內容包含好友名單、IP 位址和信任值等等資訊。

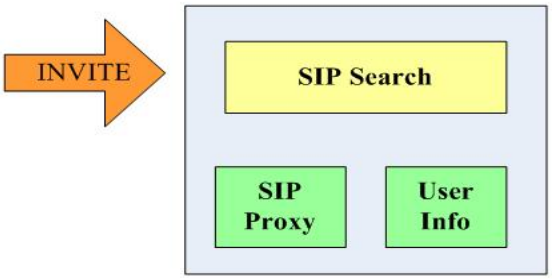

圖 4 SPITCatcher 架構

3.3 SIP Search 處理流程

圖 5 列出了 INVITE 訊息處理流程圖，當呼叫方（Caller）撥打網路電話給被呼叫方（Callee），SIP 代理伺服器接收到 Invite 訊息時，都會透過 SIP Search 來判斷呼叫方是否為一個合法的使用者。

流程說明：

1. SIP Search 收到 INVITE 訊息的時候，會先判斷被呼叫方 Callee 是否與 Caller 有直接連接的關係。
2. 如果 Callee 不是與 Caller 有直接連接的關係，則進行下一層級的搜尋，此時會針對第二層的人員做搜尋，若找不到，則再往下一層級搜尋。
3. 如果找到 Callee 則計算此路徑的信任值。
4. 查看同層是否還有其他路徑並計算其值。
5. 將找到路徑的信任等級進行比較，找出最大的信任值。
6. 將最大值的信任值與門檻值進行比較。
7. 如果信任值大於門檻值則發送 Invite 訊息到 SIP 代理伺服器並接通這通網路電話。

假設被呼叫者（Callee）與呼叫者（Caller）有間接的關係，且屬於三層以內，在透過 SIP Search 進行搜尋與處理時，不會因為搜尋過久而一直消耗資源而且降低執行的效率，且可以節省搜尋時間等等。如此，可以快速的辨識呼叫者是否為一合法的使用者。圖 6 為運用 SIP Search 的通話流程：

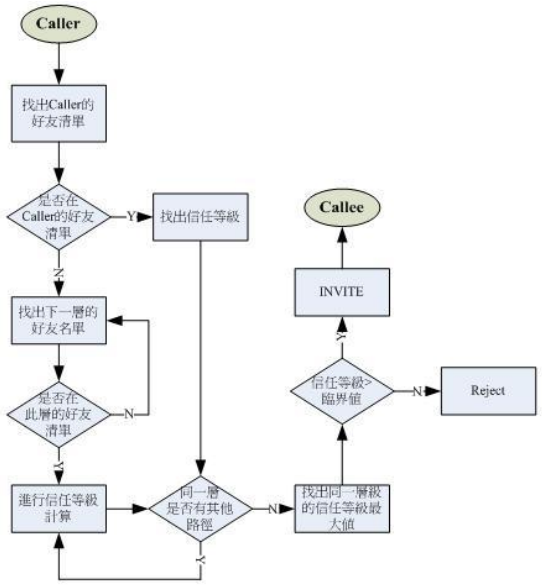

圖 5 SIP 偵測處理流程

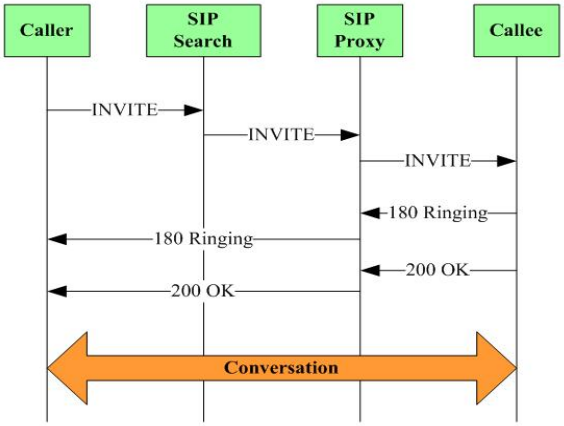

圖 6 SIP Search 通話流程圖

3.4 SPIT Manager

SPIT Manager 主要負責接收經由 SPITCatcher 所傳送的處理結果，內容包含信任等級值、呼叫者名稱和 IP 位址等等資訊，並將資訊更新至被呼叫者的清單，假使下次 SPITCatcher 再次接收到相同的呼叫者，則會直接由 SPIT Manager 將存放的信任等級值回傳給 SPITCatcher，以加速處理並且提高執行效率。

由於 SIP 是屬於即時性的服務，所以在 SPIT Manager 所記錄的資料並不會一直存在著，只會保留一個星期的時間，這主要是使用者可能隨時會改變自己好友名單的信任值，如果一直保留先前的計

算結果，有可能對方將永遠無法接通或是永遠接通，這樣就無法達到即時性的服務。

4. 系統實驗結果

4.1 系統建置

在這個垃圾網路電話偵測系統裡，我們針對 SIP 所提供的服務進行偵測。系統實驗的建置如表一所示，在量測效能方面，我們使用系統模擬程式為平台來做為本篇論文的效能測試。針對本論文的研究結果，我們將會針對 SIP 及時性的服務，進而模擬系統可以承受多少通電話，而不會發生系統延遲與效能降低並且正確的辨識合法的呼叫方。

表 1 系統架構平台

CPU	Intel Pentium 4 2.2GHz
RAM	DDR 512MB
Hard Disk	40GB
OS	Windows XP
Database	MySQL 5.0
Web Server	Apache 2.2.4

4.2 實驗結果

在實驗方面，我們定義了三種測試架構：一對多、多對一、多對多等關係。根據我們所提出的測試架構，我們模擬網路電話的通話數與正確判斷垃圾網路電話的關係，從通話數 100 開始，逐一模擬到通話數 1000，最後我們將模擬結果製作成為圖表，圖 7、8、9 是所有測試的模擬結果。

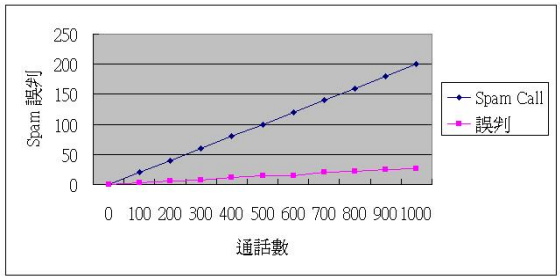

圖 7 一對多架構實驗結果

一對多架構是呼叫方設定為單一固定使用者且針對不同的被呼叫方進行通話。從這個結果中，我們可以看得出來，當呼叫者固定為單一使使用者，若被呼叫方與呼叫方是透過朋友與朋友之間的關係，則在撥打垃圾網路電話時，會視為一通合法的網路電話，而造成誤判的結果。

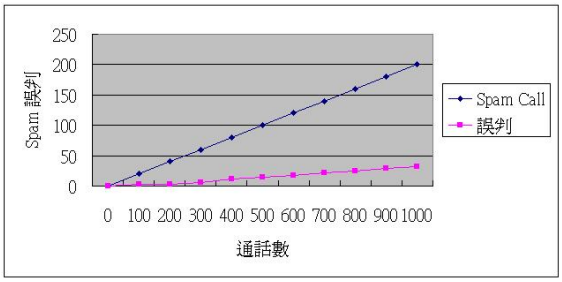

圖 8 多對一模擬結果

多對一架構是在呼叫方設定為不同對象並且將被呼叫方設定為單一固定使用者進行通話。在多對一的實驗結果中，每一位呼叫者的設定參數值都會根據他自己的喜好而有所不同，這些參數值也會影響到他撥打電話給被呼叫方的結果，因此，若呼叫方與被呼叫方是有間接的關係存在時，則垃圾網路電話將會被視為合法的網路電話，進而接通彼此雙方，形成誤判的結果。

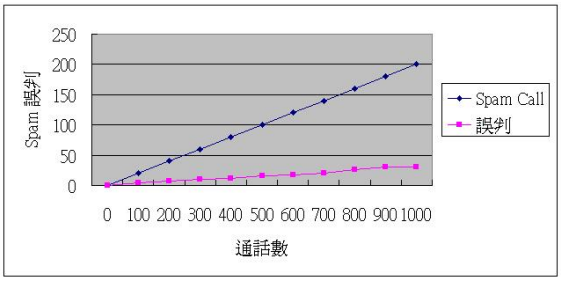

圖 9 多對多模擬結果

多對多架構是將呼叫方與被呼叫方設定為不同使用者進行通話。在這個實驗結果中，呼叫方與被呼叫方都會是不同的使用者，正因為如此，每通電話進行撥打時，會根據當時的呼叫者來搜尋與被呼叫者彼此之間的關係，這樣的條件下，彼此雙方若透過人與人之間的信任而建立關係，則撥打的垃圾網路電話將被視為合法的網路電話，並且建立雙方通話的連線，產生誤判的結果。

因此，從這些模擬結果中我們可以看得出來，

每一個功能測試都會根據使用者自己所定義的朋友信任值、搜尋層級和門檻值進行人與人之間關係的信任計算與比較，並且隨著通話數的增加，所造成誤判的通話數也只會微量的增加，這也就是說必須是呼叫者與被呼叫者之間彼此有關係存在，系統才會將垃圾網路電話誤判為合法的網路電話。

5. 結論與未來工作

目前 SPIT 對於網路電話市場並沒有太大的影響，但隨著網路電話逐漸的普遍，SPIT 的威脅將不會小於垃圾電子郵件，如此，網路電話將成為一個新興的廉價行銷管道。因此，本論文中提出了一個 SIP 服務之垃圾電話偵測系統來有效的偵測 SPIT，並且在未來，我們將會針對搜尋與計算信任等級的演算法進行改良，以達到提高效率、正確率來偵測 SPIT。

參考文獻

[1] Cao F. and Malik S., “Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure”, Proceedings of IEEE/Create-Net Workshop on Security and Quality of Service in Communication Networks, September 2005, Athens, Greece.

[2] Cao, F., “Call Filtering and Tracking in IP Telephony”, Proceeds of IASTED International Conference on Internet and Multimedia Systems and Applications, pp. 400-058, (IMSA 2003).

[3] Cao, F.; Jennings, “Providing Response Identity and Authentication in IP Telephony”, Availability, Reliability and Security, pp. 198-205, 2006. ARES 2006. The First International Conference on.

[4] Duncan J. Watts and Steve H. Strogatz, “Collective Dynamics of Small World Networks”, Nature 393, 440-442, 1998.

[5] G. Zacharia and P. Maes, “Trust management through reputation mechanisms”, Applied Artificial Intelligence, 14(9): 881-908, 2000.

[6] Jennings, C. and J. Peterson, “Certificate Management Service for The Session Initiation Protocol (SIP)”, draftietf-sipping-serts-01 (work in progress), February 2005.

[7] Larson, J., “Defending VoIP Networks from Ddos attacks”, Globecom 2004 VoIP Security Workshop, Houston, USA.

[8] Mark J. Handley, Henning Schulzrinne, Eve M. Schooler, Jonathan Rosenberg, “SIP Session Initiation Protocol, Internet proposed standard RFC 2543”, March 1999.

[9] NIST SP 800-58, “Security Considerations for Voice Over IP Systems”, pp. 800-58, 2005.

[10] Peterson, J. and C. Jennings, “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”, draft-ieft-sip-identity-05 (work in progress), May 2005.

[11] Peterson, J., “Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format”, RFC3893, September 2004.

[12] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E.Schooler, “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

[13] Y. Rebahi, “SIP Service Providers and The Spam Problem”, Workshop Proceedings, 2nd Workshop on Securing Voice over IP, Washington, USA, 01-02 June 2005.