郵件過濾個人化的設計與實作—以中央大學為例

劉劍青　　王雅慈　　曾黎明
中央大學電算中心　　中央大學資工系
center5@cc.ncu.edu.tw　　center11@cc.ncu.edu.tw　　tsenglm@cc.ncu.edu.tw

摘要

廣告信的過濾有很多文章及商業軟體及 shareware 的軟體來加以討論，中央大學基於校內使用者的需求及系統管理的需要，從民國 91 年起陸續使用 shareware 軟體，在部份使用者端試用，並於 92 年 12 月啟動第一個版本的郵件分流機制[1]，提供使用者一個共同的過濾標準，初步的判斷機制，並減緩郵件伺服器系統的壓力，然而郵件的判斷仍然必須回歸使用者的認定，每個使用者的標準不同，共同而唯一的計分標準及處理方式，無法達到滿足個人的需求，本文所提之系統為本校正式版本之第二版，以完全個人化的目標所開發出來的個人化廣告信過濾系統。本系統採用 The Apache SpamAssassin Project 開放程式碼的 Spam mail 計分引擎，使用灰名單技術、及 ClamAV 掃毒軟體，以及 MySql 等開發完成。系統特色提供許多個人化的選項，這些特性將在下面的章節介紹，本系統自 95 年 5 月正式開放以來，平均每天過濾 214791 封信，False Positives 可以達到 0.01437%。

關鍵詞：spam mail, 廣告信過濾。

Abstract

As the saying goes, “one person’s junk can be another person’s treasure”, the judgment of whether a mail is considered as a spam or not is quite different from person to person. Therefore, when it comes to spam mail filtering, it is better to let individual users to make their own decision than apply a same rule globally. In this essay, it introduces how we achieved that a server-side spam-filtering can be personalized, and how we use a bunch of open software, such as SpamAssassin and ClamAV, plus some assistant programs, including a per user greylisting facility and user interfaces, we wrote ourselves to make the whole idea into reality.

Keywords: Spam mail

1. 前言

因應病毒與廣告信件的日益增多，本校於 92 年 12 月啟動第一版的郵件分流機制系統[1]，平均每天約過濾 6-10 萬封信件，使用 Spamassassin 軟體再加上手動加 rules 的調校，以 6 分為 Spam 的標準，系統採用統一的黑白名單，並且自動分析實作自用的 DNSBL[2]及 access control，以 Webmail 讀取隔離區的信件，提供被隔離信件的摘要通知信，使用者只能選擇啟動或不啟動(其人數比為 22479:3299)，而有鑑於郵件本身屬個人認定標準不同[3]，原先的功能與架構已經不敷使用，於是著手規劃新版的過濾系統，本系統於 95 年 5 月正式啟用，結合原系統的優點，並以個人化為目標， 提供使用者可以依個人喜好及郵件特性，訂定一個適合個人的過濾系統。新系統提供的特色說明如下：

- 系統提供三種垃圾郵件處理方式: 在信件加 [SPAM] 標記、將垃圾信隔離處理、直接刪除。
- 使用者可自訂分數等級的處理方式
- 對於隔離的信件，提供摘要通知信，使用者可以直接點選通知信上的 URL 就可以直接取信。當然，使用者也可以取消通知信。
- 使用者可以自定個人的黑/白名單。
- 本系統提供《灰名單》的技術來防止 SPAM MAIL，完全依據使用者的個人意願來決定啟動與否，並非強制性的使用。
- 本系統提供十分彈性的《灰名單》啟用時段選擇，可以對一週 7 天，每天 24 小時的每一個小時做啟用或停用的設定；另外系統也提供一些預設的樣板，讓使用者快速的設定。
- 對進階的使用者，本系統提供六百多項 SPAM 檢定規則做個人化的停用 (設成零分) 或自訂分數。
- 提供使用者個人的貝氏分析 (Bayesian Analysis) 資料庫，以取代原本單一資料庫；對 Spam 的判斷更加個人化。
- 提供使用者個人的自動黑/白名單的功能。
- 對被隔離的郵件，本系統提供使用者 Web 讀取的介面，使用者可以依據日期，或 SPAM 分數排序。可將郵件下載，或直接寄回 pop 信箱。另外，使用者也可以以點選的方式將寄件者設成白名單，以確保該寄件者下次的郵件不被當成垃圾郵件。

- 使用者可以決定是不是要額外使用病毒過濾 (採用 ClamAV)

2. 系統規劃設計實作

第一版本的過濾系統，提供我們許多寶貴的回饋意見，因應全面個人化的設定，除了提供一個易懂易操作的使用者介面外，善用 Spamassassin 的應用，並加上自行開發的一些工具，提供使用者更方便的操作介面，可以減緩許多在推廣上的問題，以下就各功能面的實作加以說明。

2.1 系統硬體架構

我們採取 DNS 的 MX Record 架構(如圖 1), 可以依使用量不同，逐步擴充多台的 Spam Mail 過濾伺服器，並可隨時下線做個別的維護更新。這些伺服器上有自行開發的 perl 程式，定期檢查 MySQL 上使用者設定變更的異動表，並將有異動的設定寫在 Local 的使用者設定當中；主要包括決定不同分數不同處理方式的 .procmailrc 檔，及使用者黑白名單及進階 Spam 分數調校的 user_pref 等；由於我們控制郵件由 System space 進入 User space 時，再進行 Spam 的評分、病毒的檢查等等，所以我們可以做到高度的個人化，包括分數等級的設定，黑白名單，個人的貝氏分析表等。

Local Mailer 程式採用 procmail，利用使用者的 .procmailrc 檔，我們可以把使用者信件先丟進 Spam Assassin 做 Spam 的計分，Spam Assassin 將在原信件的 Header 部份註記 Spam 分數。接下來 procmail 可以依 Spam Assassin 的計分，以及使用者的設定，決定該封信的流向。Spam 信件則送往隔離區，而正常信件則丟給 Virus Scan，沒問題的信件會通過 Virus Scan 而進入使用者信箱。

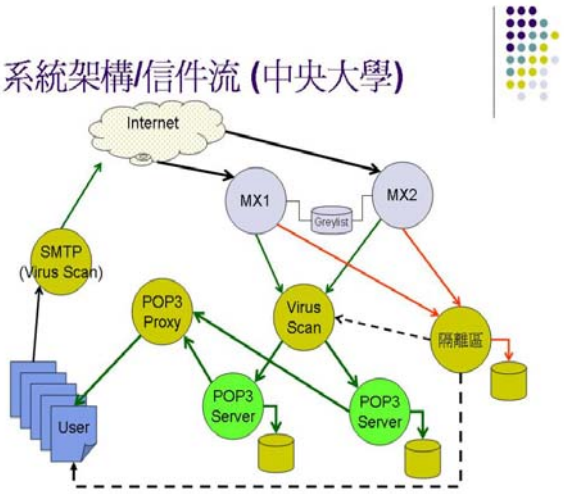


圖 1 系統硬體架構

2.2 軟體開發設計

- ✓ 作業系統: Fedora Linux Core 4 / Core 5
- ✓ 計分引擎: SpamAssassin 3.0.x / 3.1.x
- ✓ 網頁伺服器: Apache 2.0.x + PHP 5.x
- ✓ 工具程式: procmail, mrtg
- ✓ 郵遞軟體: sendmail
- ✓ 資料庫使用: MySQL 4.1.x
- ✓ 自行開發的部份：

sendmail 的 filter 程式: 做灰名單用 (C)

網頁讀信/設定/管理程式 (php)

其它整合用的小程式 (C, Perl)

2.3 系統功能實作說明

為了收集使用者的個人意願設定，撰寫一個網頁形式的設定介面讓使用者可以去設定個人的喜好，並將這些設定結果儲存在 MySQL 的資料庫中(如圖 2)。

圖 2 使用者設定劃面

2.3.1 根據使用者在介面上設定的資料，幫他寫入 SpamAssassin 的使用者設定檔 ~/.spamassassin/user_pref

例如使用者啟動等級 1 分數為 2，並在信件主旨加上[SPAM]，對於進階設定中的 RCVD_IN_BL_SPAMCOP_NET 這個選項調校為 4 分，並加上一個白名單 perter_pan@neverland.net

```
required_score      2.0
rewrite_header subject [SPAM]
score RCVD_IN_BL_SPAMCOP_NET      4.000
whitelist_from      perter_pan@neverland.net
```

2.3.2 善用 procmail 的使用者設定 ~/.procmailrc 例如使用者啟動 5 分隔離, 8 分刪除的功能

```
:0fw
| /usr/bin/spamc
:0
* ^X-Spam-Level: \*\*\*\*\*\*\*\*      =>8分直接刪除
/dev/null
:0 w
* ^X-Spam-Level: \*\*\*\*\* =>5分送到隔離區的主機
| /usr/local/sbin/relaymail user@detention.xxx.edu.tw
```

```
:0 w          ===>直餘送件送到正常 pop3 server
| /usr/local/sbin/relaymail user@pop.xxx.edu.tw
```

2.3.3 如果是 IMAP Server, 可以直接丟到 SPAM 的郵件匣 (本例為 2 分)

例如使用者如果使用 IMAP 收信，可以加以控制將信件放到不同的資料匣

```
:0fw
| /usr/bin/spamc
:0
* ^X-Spam-Level: \*\*\*\*\*\*\*\*\*\*  ===>8 分直接刪除
/dev/null
:0 w
* ^X-Spam-Level: \*\*\*\*\*           ===>5 分送到隔離區的主機
| /usr/local/sbin/relaymail user@detention.xxx.edu.tw
:0 w
* ^X-Spam-Level: \*\*
| /usr/bin/dmail user+SPAM           ===>2分將信件放在某一資料匣中
```

2.3.4 因應本校帳號編碼的關係，與 spamassassin 的 rule 有所衝突，所以我們做了一些調整：

如果帳號結尾有二個以上的數字 – 可能會得到 FROM_ENDS_IN_NUMS 這項分數

例: center5 (ok)
center11 (From ends in numbers)

如果用學號當 Email 帳號 – 可能會得到 FROM_ALL_NUMS,FROM_STARTS_WITH_NUMS

因此我們為此做了一些分數的補償

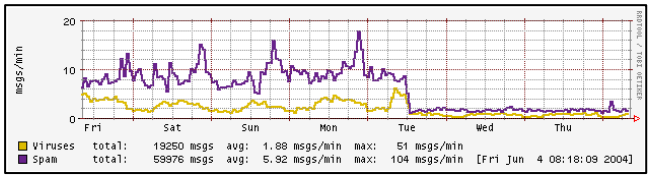
```
header FROM_NCU_STUDENTS
  From:addr =~ /\d{7}\@(cc\.)?ncu\.edu\.tw/
describe FROM_NCU_STUDENTS          From: sender is a student

score FROM_NCU_STUDENTS             -5.000
```

2.3.5 灰名單個人化的實作：

灰名單[5]的技術在很多文章中都有提到其效益,簡單來說, 灰名單的技術是利用正常 Mail Server 重送的特性, 利用延遲接受法, 有效的阻止垃圾郵件; 但是有很多的電子報或銀行的通知信會被灰名單的技術阻檔於外，主要原因是這些軟體並沒有遵循信件無法成功投遞時應該啟用的正常步驟，這使用得啟用灰名單會造成遺失信件的機率增加許多，基於此本系統所提供的灰名單技術不但做到個人可自行決定是否啟動，更進一步做到使用者可以依個人習慣在 7 天 24 小時共 168 個時段來決定啟用灰名單隔離垃圾信與否;這可以讓使用者決定在上班時間不想要延遲收信的功能，但是在下班後，則可以啟動這個功能以杜絕廣告信的來源。

在實作的部份，使用者設定介面的部份，仍是以 php 開發的 web 程式來處理. 灰名單所使用的工具是自行研發的, 它是一個以 C 語言撰寫的 Sendmail Filter, 以 Connection pool 的方式連接後端 MySQL 資料庫, 去檢查使用者啟動與否? 該封信是否已通過灰名單測試? 該信的寄件者是否在使用者白名單所列等等。更重要的是, 這個 Sendmail 在設計上是 Fail Safe 的, 也就是說, 如果資料庫連結有問題或程式有異常等, 它會 by pass 灰名單的檢查, 以防止使用者掉信，自行開發的 Sendmail filter 在 sendmail.mc 加 INPUT_MAIL_FILTER(`sm-grey', `S=unix:/var/spool/smf/sm-grey.sock, T=S:30s;R:1m')，其工作原理主要是在 MySQL 資料庫中放有啟用的帳號的啟用資訊, 包括 7 個欄位的整數分別代表週日至週六每天 24 小時是否 Enable 的 bitmap，這個 sendmail filter 程式取出 MySQL 資料庫中 receiver 在該天的整數 bitmap 值。取不到, 表使用者未啟動; 取到的話, 則用現在的時間去做如下的運算 day0 & (1 << hour), 如果得到非零, 表這個時段使用者要使用灰名單, 接下來就照一般的灰名單處理。

由於灰名單對我們的系統而言，並不是強制使用，所以無法看出其整體效率，下面這個圖表是 postgrey 網站宣稱的效果



下表是觀察我們系統上某用戶使用前及使用後的狀況 (6/2 晚上)

日期	5/27	5/28	5/29	5/30	5/31	6/1	6/2	6/3	6/4	6/5	6/6
Spam	188	194	188	206	192	137	126	26	18	19	18

2.3.6 對於隔離的信件, 提供摘要通知信, 使用者可以直接點選通知信上的 URL 就可以直接取信。當然, 使用者也可以取消通知信，這個功能是由一支自行開發的 perl 程式, 分日期、分使用者, 一封一檔的方式儲存在檔案系統中, 並把一些檔頭的資訊存在 MySQL 資料庫中; 使用者可以利用 Web 介面(php 程式)登入系統瀏覽取信, 或由系統每天匯整該天的隔離信件以 Email 寄一個匯整表給使用者(perl 程式), 在匯整表上

包括 URL 的連結，使用者可以方便的撈回誤判信件

3. 系統上線推廣

系統設計完成，經過測試及準備文件預定開放使用，最大的問題在於新系統的初始值應該給多少？這是一個最讓系統管理者頭痛的問題，因為這個系統是一個需要使用者互動的系統，上線初期必須面對使用者的詢問，調校的不穩定及信任感，如何在一開始即讓使用者感受其優點，再依個人特色去調整是一個最大問題，如果不能讓使用者一開始即感受到這個新的過濾系統比第一版本更有效率，那麼就無法順利推廣，所以我們決定以較嚴格的設定為初始值，以突顯新系統的特色，再局部對於不熟悉系統的使用者，做個別的調校諮詢服務，因此系統的管理介面非常重要(如圖 3)，提供從網頁即可直接查詢使用者的設定值，在推廣初期，對於不是很了解此系統的使用者，可以透過電話即可了解問題及直接代為設定，減少許多的不安。

新系統的上線，還包括穩定性的需求，全面個人化後系統以不同的條件判斷時，與第一版本的共用 profile，其對系統的負荷問題，都會是系統上線的最大考驗，因此新系統上線採用漸進式，以確保系統移轉時的穩定性，所以在 5/24-5/31 之間，信件的過濾是採用新舊系統並用，負載平衡的原則下進行，只是判斷信件是否為 spam 的標準不同，這提供我們觀察系統是否已超過負荷，並機動調整我們事先沒有考慮的因素，除了事前已經透過許多型式的公告，在網頁上提供許多新系統的常見問題及建議外，上線後觀察期每天都有系統狀況報告及小技巧的建議，同時系統提供許多統計資料及流量圖，讓使用者及管理者了解並透明化資訊，包括圖 4 的使用者設定統計資料、圖 5 的 Spam 隔離件數、圖 6 的 False Positives 數量、圖 7 的 Spam 流速。

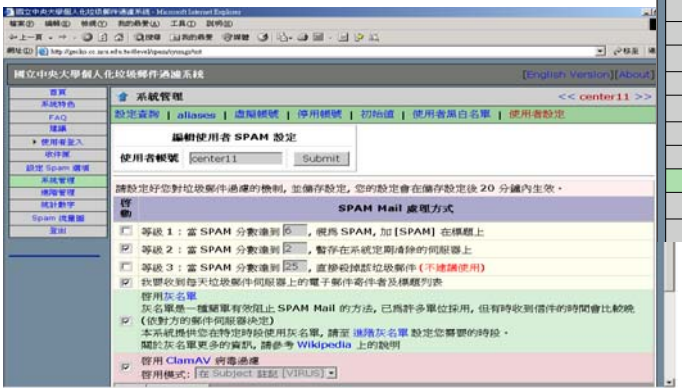


圖 3 系統管理介面

圖 4 使用者設定統計資料

圖 5 Spam 隔離件數

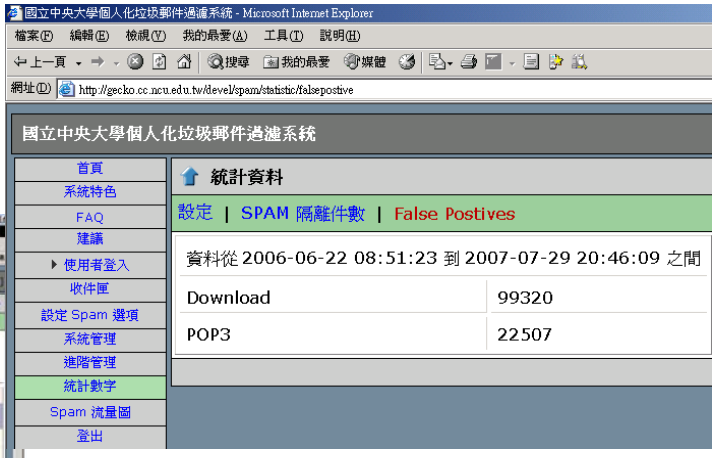


圖 6 False Positives

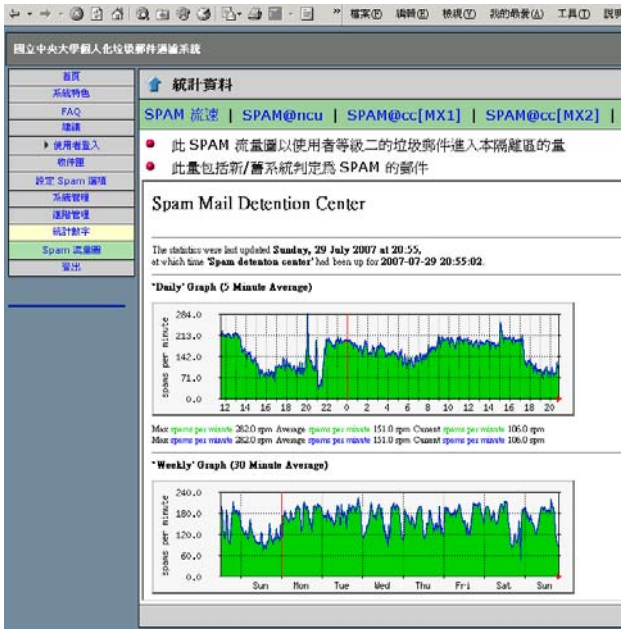


圖 7 Spam 的流速

4. 結論與展望

本系統自 95 年 5 月開放以來，沒有做特別的調校，只有陸續對於使用者的操作問題加以說明，本系統網址為 http://spamconf.cc.ncu.edu.tw，除了需要進入調校設定外，使用者可以直接從通知信中取得誤判的信件，所以大部份使用者並不需要進入此系統。系統提供的一個線上的簡易版服務滿意度調查，截至目前為止有 412 人投票，平均值為 4.034 顆星(最高為 5 顆星)，從過濾的總信件數及被認為誤判而取回的信件數(包括直接從通知信中下載及從網頁寄回信箱)，這個 False Positives 數達到 0.01437%，雖然廣告信的技術層出不窮，過濾廣告信這件事也必須隨著潮流不斷在改變，但是本系統所研發及建構的個人化郵件過濾系統，對於使用者及管理者仍然是一個非常重要的平台，並以這個平台，繼續延伸提供使用者更好的選項及條件來協助使用者管理及調校過濾的方法及條件。

由於目前本系統並沒有提供回饋的機制，雖然採用個人化的貝氏分析資料庫，但卻沒有辦法調校屬於個人的貝氏分析法。也由於這個缺乏，我們在計算 False Positives 是採用計算使用者由隔離區撈回郵件的事件做計算，並不考慮使用者實際認定；另外，我們也完全無法計算 False Negatives 的情形，這會是本系統將來應該深入探討的部份。

參考文獻

[1] 王雅慈、張慈敏、劉劍青、曾黎明、陳奕明,"Spam/Virus Mail 分流機制探討—以中央大學為例", 2004 年台灣網際網路論文集
[2] 王雅慈、曾黎明、游象甫、陳奕明,"廣告電子郵件的分流過濾及回覆訊息之萃取",2005 年台灣網際網路論文集
[3] 劉大川、陳昌盛、葉育如、葉致偉、林嘉軒、薛良斌,"可擴充之電子郵件系統建構與個人化郵件過濾機制",2002 年台灣網際網路論文集
[4] SpamAssassin 網站 http://spamassassin.apache.org/
[5] 灰名單 http://www.greylisting.org/
http://projects.puremagic.com/greylisting/whitepaper.html
http://isg.ee.ethz.ch/tools/postgrey/