一個防廣告信件及內容過濾之整合系統架構

陳志明 余興華 陳朝欽
清華大學資訊工程所
E-mail: g936321@oz.nthu.edu.tw

摘要

目前電子郵件系統面臨最大的問題便是垃圾郵件氾濫以及病毒郵件的傳播，對於這些垃圾郵件的防堵以及病毒信件的偵測，市面上已有不少軟體在研究發展之中，但其中不乏功能不佳或執行效能緩慢的系統，又這些過濾偵測的機制大多在郵件伺服器上執行，反而增加系統負擔，拖累系統效能，進而更可能會遭受大量的垃圾郵件攻擊而癱瘓系統，所以提出一個可行簡便，多重過濾的系統，目的在於增加判別廣告信的辨識率以及研究在個人電腦上能有效阻擋垃圾信件以及病毒的方法，系統中除了使用黑名單（Black List）、白名單（White List）、信件格式過濾，和信件內容過濾四個部分，其中內容過濾主要擷取廣告信常出現的詞彙當作特徵，利用使用者已判定為廣告信的內容作為訓練（training）的樣本，使得系統內容過濾所擷取的特徵會越來越趨向使用者的認定標準，進而提升辨識率，以達到阻擋垃圾郵件的目的。

關鍵詞：垃圾郵件、廣告信件

1.前言

垃圾郵件在目前而言還沒有一個非常嚴格的定義。一般而言，凡是未經用戶許可就強行發送到用戶的郵箱中的任何電子郵件就稱為垃圾郵件，通常這些郵件內容包羅萬象，如賺錢信息、商業或個人的網站廣告、成人廣告、電子雜誌、產品宣傳，甚至是連鎖信，這一類垃圾郵件具有大量發送的特徵。垃圾郵件可以分為良性和惡性的。良性垃圾郵件是各種宣傳廣告等對收件人影響不大的信息郵件。惡性垃圾郵件是指具有破壞性的電子郵件。而要探討如何防堵垃圾郵件之前必須對電子郵件進行管理上的定義，簡單而言可依照使用需要性分成 White Mail、Spam Mail 及 Gray Mail 三個等級:

- White Mail 即公務性收發信件及同意收信的電子郵件。
- Spam Mail 通常具有偽造寄件人、偽造收信人或大量傳送…等特徵，使用者並不想收到的電子郵件。
- Gray Mail 垃圾郵件不能單靠特徵進行定義，若從內容需求性來看，往往在不同時間或不同環境下就會有不同的判斷，而這就使得此類信件產生模糊不清的灰色地帶，所以當廣告郵件的內容上關係到使用者需求或認知上的差異，就變成灰色地帶的垃圾郵件。

以現在來看大部分的垃圾郵件過濾系統大致可以分成兩類:

- 主張透過信件的 Header、發送模式…等 Spam 行為特徵來判斷，進而信件通過或是直接丟棄，但是這一大類對於 Gray Mail 並沒有顯著的改善。
- 主張以內容過濾、語意分析…等深層過濾技術可解決灰色地帶垃圾信件的問題，目前常見的混用多種過濾技術，即黑名單、白名單、規則過濾法 (Rules Filter)、內容過濾法 (Content

Filter)、路徑偵測法(Detect Routing)、貝氏過濾法(Bayesian Analysis)…等技術

一般而言防堵垃圾郵件的難度在於，垃圾郵件發送者經常變換發信地址、偽造發信地址、利用程序隨機挑選變換郵件內容，這些使得防堵垃圾郵件的難度變得更高，從技術的角度來講很難做到完全根除垃圾郵件。

所以在這裡我們討論的系統將使用多重過濾的原則，透過簡單的格式辨別的方法，以及計算廣告信特徵值，來判別是否為廣告信件，其中系統的流程以及判別策略將在第二章簡述，而第三章則描述未來可探討研究的方向。

2.防廣告信及內容過濾之系統架構

系統中採用多重過濾原則，主要分為四個部分，白名單、黑名單、信件格式過濾機制以及信件內容過濾機制來偵測廣告信件（如圖 1）。

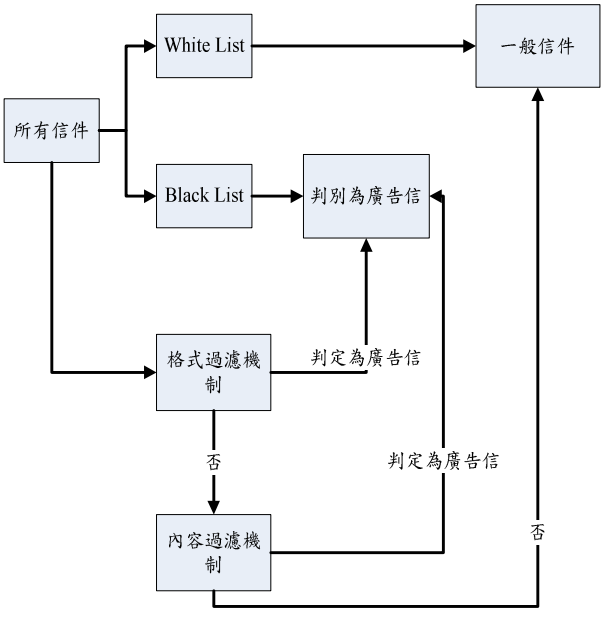

圖 1 防廣告信與內容過濾系統架構圖

2.1 白名單（White List）

白名單為記錄使用者許可的傳送來源，此類信件則不經黑名單、格式和內容過濾的機制，通常為使用者願意收到的廣告信或者是一般的信件往來，系統可以藉由使用者所設定的通訊錄來得到此份名單，並可由使用者自由增減。

2.2 黑名單（Black List）

黑名單為記錄使用者不願收到的信件來源，此類信件也不經格式與內容過濾，直接判定為廣告信件，可以增加系統過濾效率，此名單可以從使用者所判定的廣告信得到，也可由使用者自由增減。

2.3 格式過濾機制

此部分功能針對郵件的格式作為判斷的依據，分為寄件人地址格式、偽造來源端、偽造寄件人位址利用這些特徵來辨別廣告信，如圖 2。

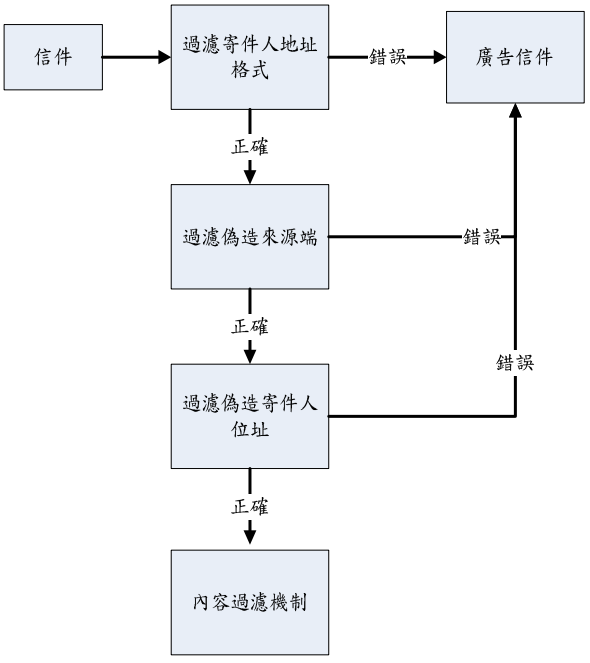

圖 2 信件格式過濾系統流程圖

2.31 過濾寄件人地址格式

廣告信的發信人位址有時候格式不正確，我們可檢查這部分信件格式，藉由這部分可以過濾部分的垃圾信件。

2.32 過濾偽造來源端

廣告信件的發信主機通常會試圖隱藏自己的來源，或者偽造其他假名來，藉由這部分的信件格式檢查，我們可以過濾掉大部分的垃圾郵件。

2.33 過濾偽造寄件人位址

檢查 E-mail 上信封以及信件的發信人位址是不是相符合，廣告信件通常有不相符合的情形產生。

2.4 內容過濾機制

內容過濾機制採取廣告信中常出現的字彙當作特徵值，若接收信件的特徵值與廣告信的特徵值相符合的個數相當高，系統則判定此信件為廣告信件，並將這廣告信的特徵值（常出現的字彙）加入到系統擷取出的廣告信特徵資料庫中，而一開始廣告信的認定，由使用者來判讀，或者經由格式過濾機制所判斷出的廣告信件，來當作訓練過濾系統的樣本廣告信，藉由不斷的訓練之下，系統會越來越趨近使用者的要求。

而在病毒郵件部分，若是惡意的垃圾郵件含有病毒，將採用外掛的防毒軟體來檢查這一部份，因此我們將未判斷的信件先經由外掛的防毒軟體偵測出是否有病毒，若有病毒則直接刪除，否則才進入內容過濾的系統，確保在判斷的過程中沒有病毒的威脅。

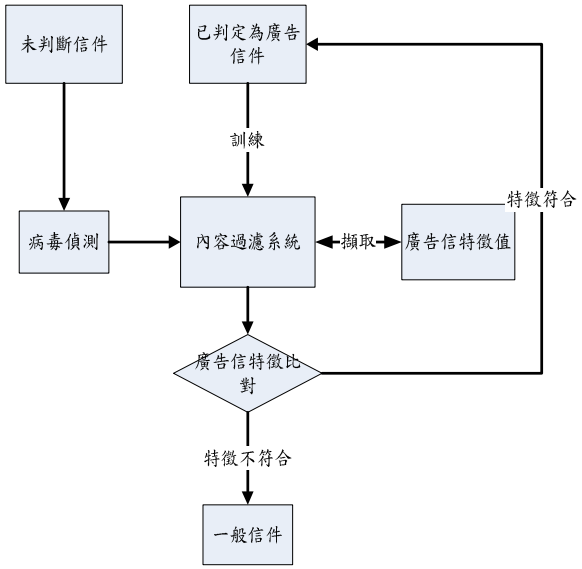

圖 3 信件內容過濾系統流程圖

3.討論與未來方向

大量氾濫的廣告信件已經是電子郵件系統所面臨到的最大問題，大量的郵件不但會耗用的網路頻寬，更使得網路信箱無緣無故被廣告信塞滿，佔用使用者的許多時間和精神，為了防堵各種日新月異的廣告郵件，市面上的信件軟體也不斷研究更精準的判讀方法，但大多數的軟體，在更精準的情況之下，也越消耗系統的資源，所以在未來的工作裡，可以朝研究內容過濾的演算法，加強字串比對演算法的效率，以及支援更多信件流通的協定，同時藉由更多的協定來偵測廣告信，另一方面也可加強硬體的支援，加速系統的效能，達到確實防堵廣告信件的目的。

參考文獻

[1] Bayes' theorem, http://www.absoluteastronomy.com/encyclopedia/B/Ba/Bayes_theorem.htm

[2] Cisco, http://www.cisco.com .

[3] Check Point, http://www.checkpoint.com .

[4] FortiNet, http://www.fortinet.com .

[5] Graham, Paul,"Better Bayesian Filtering", http://paulgraham.com/better.html January 2003.

[6] ISS, http://www.iss.net .

[7] NetScreen, http://www.netscreen.com .

[8] Symantec, http://www.symantec.com/index.htm .

[9] Trend Micro, http://www.trendmicro.com .

[10] WatchGuard, http://www.watchguard.com .

[11] WebSense, http://www.websense.com .

[12] 蔡均璋(2004)，垃圾郵件防制宜日新月異，PC Week 電腦週報，(701)，61。

[13] 畢建同(2003)，導入 Anti-SPAM 測試要訣，有效反制垃圾郵件 [線上資料]

[14] C. Ding, C. Chi, J. Deng, and C. Dong, "Centralized Content-Based Web Filtering and Blocking: How Far Can It Go?," IEEE Transaction on System, Man, and Cybernetics, vol. 2, pp. 115-119, October 1999

[15] Geoff Hulten,Joshua Goodman and Robert Rounthwaite(2004),"Filtering spam e-mail on a global scale," In Proceedings of theThirteenth International World Wide Web Conference, New York, pp. 366-367.

[16] R. Knobbe, A. Purtell, and S. Schwab, "Advanced Security Proxies: An Architecture and implementation for High-Performance Network Firewalls," Proceedings of the DARPA Information Survivability Conference and Exposition, vol. 1, pp. 140-148, January 2000.

[17] J. Klensin, Editor. Simple Mail Transfer Protocol. Request for Comments 2821, Internet Engineering Task Force, April 2001

[18] S.J. Saving, Vaughan-Nichols Private E-mail. Spectrum, IEEE, August 2003, 40-44.

[19] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz. A Bayesian approach to filtering junk email., AAAI Workshop on Learning for Text Categorization, July 1998, Madison, Wisconsin. AAAI Technical Report WS-98-05