從眾行為在不當資訊防制上的應用

王鐵雄　陳思翰　蔡顯明　林俊男　李新林
國立中正大學電子計算機中心
E-mail: {tswang,shchen,tsices,cnlin,singling}@ccu.edu.tw

摘要

目前關於不當資訊防制的相關研究，大多著重在關鍵詞庫或圖形比對等技術面的觀點，本文則是著眼於制度面的角度，以 TANet 現行階層式管理架構為基礎，提出一套整合區域內各單位資源的聯防機制，在不需要增加人力及經費的前提下，透過簡單且易於實現的機制，以最小的成本達到最佳的防制效果。本研究主要是以網路從眾行為的觀點，設計一套不當資訊黑名單資料庫管理維護系統，希望在不影響下層單位的系統效能的情況下，以最少的記錄筆數達到最大的防制效果。經過實際測試並收集相關的記錄檔加以分析，結果發現本研究所提出的防制機制，的確能夠發揮預期的效果，大幅降低不當資訊的流量，並減輕上層單位的負荷。

關鍵詞：從眾行為、不當資訊、黑名單。

1.前言

根據專門開發網站過濾軟體的 N2H2 公司在 2003 年 9 月 23 日發佈的報告指出，目前網際網路上的色情網頁已經暴漲到 2 億 6,000 萬個，這和該公司 1998 年的資料庫中可確定的色情網頁 1,400 萬個來相比較，短短的五年中竟然暴增了 18 倍 [1]。此外，根據追蹤網路用戶上網習慣的市研機構 Hitwise 於 2004 年 5 月 29 日截止的當週調查發現，訪客量較高的五大網站類別（如圖 1）中，色情成人網站訪客到訪率高居各類網站之首，包括 Google、Yahoo Search 和 MSN Search 在內三大蒐尋引擎網站訪客量還不及色情網站的三分之一。根據 Hitwise 統計，當週美國各類網站訪客量占所有網站訪客量的比例，以色情網站最高占達 18.8%，蒐尋引擎及目錄類網站占 13.8%居次，其他各類網站：娛樂類網站 8%、商業暨金融類網站 7.4%、購物暨分類廣告類 7% [2]。從 N2H2 及 Hitwise 等機構的研究報告來看，就可以知道目前網際網路上色情問題的嚴重程度。

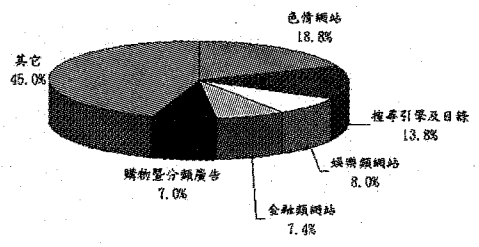

圖 1 各類網站訪客量比例

台灣學術網路 (TANet) 是教育部主導的學術研究網路，連線單位遍及全國各級學校及學術研究機構，除了提供給學校教職員工做為教學、研究及行政支援的用途之外，同時也是各級學校的學生上網的主要場所，由於大多數學生身心發展尚未成熟，對事情的是非對錯仍缺乏獨立判斷的能力，如果長期處於不良的資訊環境中，很容易產生價值觀的扭曲，造成無可挽回的後果。

因此，為了避免 TANet 遭到不當資訊的污染，讓學生可以在純淨的網路環境下，快樂而安全的上網學習，台灣學術網路管理委員會特別成立「台灣學術網路資訊使用管理小組」，並分成北中南三個分區推行一項為期三年的不當資訊防制計劃 [3]，本中心和成功大學及中山大學負責南區不當資訊防制的整合計畫。此一計畫分別在北區購置十五套高性能不當資訊防置設備、中區購置十套、南區購置十二套；三年耗費的軟硬體及不當資訊黑名單資料庫的更新費用高達數千萬元，這對於日益困窘的教育經費而言，無疑也是一筆沉重的負擔。

有鑑於此，本中心乃利用從眾行為的觀點設計一套以區域網路中心為範圍的不當資訊聯防架構，由區網中心建立一套不當資訊黑名單資料庫管理系統，讓下游學校可以在不需要增加人力及經費的情況下，協助進行不當資訊的初步攔阻，以減少網路流量，並降低上游代理伺服器及不當資訊防制設備的負擔，如此不僅可以達到不當資訊防制的目的，同時能提高系統的穩定性，並維持網路的服務品質，同時也能大幅降低不當資訊防制的成本。

2.從眾行為

從眾行為是一般日常生活中非常容易出現的情況，諸如人云亦云、追求時尚流行、一窩蜂搶購蛋塔、… 等等，這些都是所謂的從眾行為。個人在群體中與他人互動免不了會受群體的影響，而在行為上或思想上有所改變。一般所謂之從眾可分為二個層次：順從輿論 (public compliance) 和私下接納 (private acceptance)。「順從輿論」是指，個人雖然採取了符合群體期望的行為，但內在的信念並沒有改變；而「私下接納」則是，個人的信念與行為都受到了群體的影響，因而改變與群體相一致 [4]。

有關從眾的研究最早是出現在 Solomon Asch 的研究中 [5][6][7]。Asch 當時並沒有明確界定

「conformity」的定義，因此未成為一個專有名詞，其所提及與從眾涵意相似的名詞為「多數效果(majority effect)」。Asch 的文章發表後即引起許多社會心理學者的興趣並深入探討從眾的現象及發生的原因，同時也引發社會學、行銷學等其他領域的專家的觀察並應用從眾行為。各個領域對從眾所持的概念相似，但重點不太相同。本研究是以網際網路中的虛擬社會為研究標的，因此採用社會心理學領域的定義：「從眾為社會的影響表現，其影響來源為個人受到團體中其他成員的影響」。

Hanson 和 Putler [8]在免費軟體網站上做了一個實驗，針對兩個相似性質的檔案，竄改其中一個的下載次數，結果發現使用者會以下載次數這個指標做為品質考量的依據，亦即使用者會大量湧向熱門（下載次數多）的軟體，而下載次數高的項目會吸引更多的使用者，而形成「大者恒大」的效果。這個實驗除了說明下載次數為使用者的品質衡量指標，也證實了網路上的從眾行為確實存在。

另外一個證實網路上從眾行為的實驗，對象為在網路聊天室中一群互不認識的受測者，內容則與 Asch 的實驗相似，即測試四條線中哪一條線與另一條基礎線等長，除了受測者之外聊天室中的其他成員皆為事先安排好的，實驗結果證實了即使在匿名的網路上，人們仍然如同真實世界般，會受到同儕壓力的影響，即使群體的意見明顯是錯的 [9]。

在網際網路上諸如此類的例子相當多，以搜尋引擎及分類目錄為例，根據 Hitwise 的調查發現，美國三大搜尋引擎及分類目錄分別為 Google、Yahoo Search、MSN Search，而這三者的訪客量幾乎是其它眾多搜尋引擎及分類目錄網站的訪客量的總和。此外，像是拍賣網站的 eBay、Yahoo，或是網路書店的 Amazon，這些網站的訪客量一直是居高不下，其它網站則難望其項背。而在其它各類型網站也同樣都有此大者恆大的現象。由此可知，網際網路上人們同樣的會有從眾行為的發生，而本研究即是根據此一觀點，將從眾行為應用於不當資訊的攔阻上，利用各不當資訊網站從眾性的高低做為不當資訊攔阻清單的決策依據。

3.不當資訊防制機制的設計

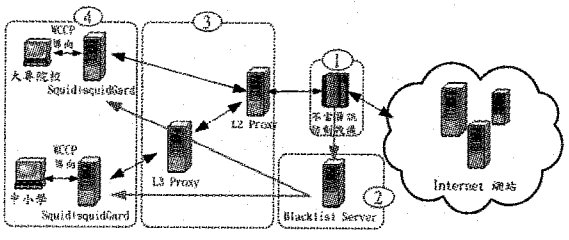

圖 2 本研究提出的階層分工架構圖

在本研究架構中(如圖 2)，主要是由：(1) 不當資訊防制設備、(2) 不當資訊清單伺服器 (3) 區域網路中心及縣市教育網路中心 (4) 下游學校等四個部份所組成，各部份負責的功能分述如下：

3-1 不當資訊防制設備

由區網中心負責購置高性能的不當資訊防制設備一套，負責進行全面性過濾攔阻的工作，此不當資訊設備具備之功能包括：

1. 在網路骨幹端 mirror 使用者所發出的 http request，以進行檢查的工作。

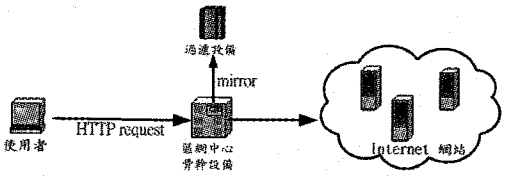

圖 3 將 request mirror 到防制設備

2. 若此瀏覽要求之網址存在於不當資訊防制設備內建的不當資訊資料庫中，則拒絕該筆瀏覽的要求，一方面送出中斷訊息給被瀏覽之網站，令其不需傳送網頁內容；另一方面將 request 導向訊息回應之網頁，送回給拒絕網頁連線通知給使用者。

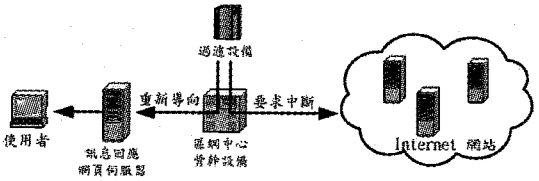

圖 4 不當資訊攔阻示意圖

3. 若此瀏覽要求不存在於過濾器內建的不當資訊資料庫，則由網站傳回網頁給使用者，完成瀏覽過程，不當資訊防制設備針對傳回的網頁進行 mirror 並進行網頁內容分析，以判斷是否為不當資訊之網頁。

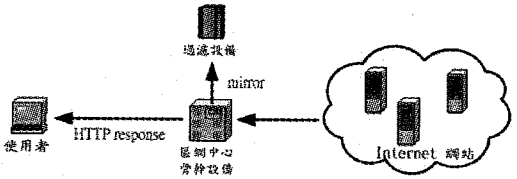

圖 5 將網站回應內容 mirror 到防制設備

4. 經步驟 3 判定為不當資訊之網頁，則自動加入不當資訊黑名單資料庫，以動態增加不當資訊攔阻的黑名單。

3-2 不當資訊清單伺服器

由區網中心負責建置一部不當資訊清單伺服器，由於此伺服器只需負責不當資訊清單的建置及管理維護，因此只需用一般電腦主機即可勝任，不需要另外再購置高階伺服器主機。

3-2-1 不當資訊清單之建立

基於商業利益的考量下，不當資訊防制產品的黑名單資料庫是屬於該產品的主要價值之一，因此，大多會經過編碼處理，以防止別人取得該資料庫之內容，此外，這類經過收集而得到的完整資料庫亦屬於智慧財產權保護的範圍。基於以上的因素，我們無法直接從不當資訊防制產品中直接取用其不當資訊黑名單資料庫。

因此，本研究乃根據教育部所提供的三萬餘筆的不當資訊清單以及 squidGuard.org 所提供的十三萬餘筆的不當資訊清單，排除 ads, proxy, warez, mail 等不在台灣學術網路認定為不當資訊的類別以及兩者重複的部份之後，彙整而得到基本的不當資訊黑名單，總計十萬餘筆記錄。

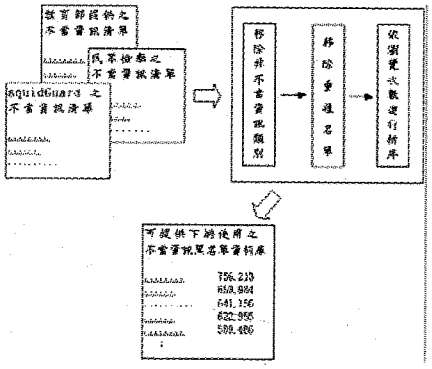

圖 6 不當資訊黑名單之建置示意圖

在本研究中，我們主要是以網路從眾行為的理論為基礎，並根據四月份從雲嘉區域網路中心及嘉義縣市教育網路中心收集到 Proxy Server 記錄檔共5億9千萬餘筆記錄加以統計排序，而得到本研究所需要的不當資訊黑名單清單。由於本清單已針對各不當資訊網站被 request 次數進行排序，因此可以利用排名較前面的清單提供給下游學校使用，下游學校只需針對這份排行榜前面的清單進行初步攔阻，如此一來即可解決下游學校各自搜集不當資訊清單的困擾，同時也能在不造成系統負擔的情況下達到非常高的攔阻效果。

3-2-2 不當資訊清單之新增

在建立不當資訊黑名單基本資料庫後，接下來的問題是如何有效增加近期瀏覽次數排名較高的不當資訊網站。本研究利用不當資訊防制設備所提供的每週 Top 300 的不當資訊網站存取排行做為判斷及新增不當資訊黑名單資料庫的依據，並撰寫一個 parser 模組負責擷取 Top 300 網頁中的網址及瀏覽次數。然後再和現有不當資訊黑名單資料庫進行比對，若為重覆網址則將次數累加至該網站的瀏覽總次數，若為新的不當資訊網頁，則將該網站之網址及瀏覽次數新增到不當資訊黑名單資料庫中。將瀏覽排名 Top 300 的網址的 parser 模組:

```
#!/bin/csh
set list=/tmp/list.abuse
set SquidGuard="./squidguard"
cd /home/data

// fetcher
wget -m -L -l 0 -t 0 -A html -X xkmgr/icons
     http://192.83.190.229/xkmgr/

// transform
find ./ -name TUW\*html -print > $list
awk '{print "lynx -dump -raw "$1,$2" |grep ://|grep -v \\|
     |./print_url >
     squidguard/urls."substr($0,length($0)-25,21)}' $list |sh
cat $SquidGuard/urls.* |sort -u >$SquidGuard/URLs
```

每天可利用 crontab 自動執行，減少人工作業:

```
5  0  *  *  7  /root/parser
```

此方式的優點在於不須耗費人工去收集不當資訊清單，而且可以由系統每週自動進行，亦不需要耗費太多的管理人力，同時又能兼顧到近期較熱門的網站的攔阻效果。因此，這種方法可以用最低的成本而得到最大的防制效果。

3-2-3 移除不存在之網站

在本研究中，我們使用 GNU 的 wget 程式進行擷取測試，如果擷取失敗則判定為無效網頁，而從不當資訊黑名單資料庫中予以移除。

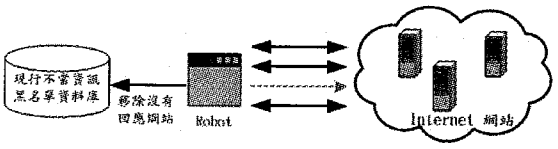

圖 7 移除不存在之網站清單示意圖

在本研究中，我們撰寫一個簡單的 PHP 程式來進行檢查，其呼叫 wget 之用法如下:

```
$ret = system(wget -q -i list_file -t 3 -T 10
--delete-after);
```

每月利用 crontab 自動執行，減少人工作業:

```
20  0  10  *  *  /root/drop.php
```

3-2-4 餵送下游單位之機制

區域網路中心的不當資訊清單伺服器和下游各學校之間可以使用 rsync（遠端檔案同步）做為自動傳送的機制。rsync 在 Linux 系統安裝時通常以預設為安裝，因此不須要再額外安裝，只須作好設定並啟動即可。在使用 rsync 時，Server 端和 Client 端必須先做好必要的設定以便傳送檔案。

1. 設定 /etc/xinetd.d/rsync

```
#default: off
# description: The rsync server is a good addition to
am ftp
# server, as it service rsync
{
        disable         = no
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/bin/rsync
        server_args     = --daemon
        log_on_failure  += USERID
}
```

2. 啟動 rsync

將 rsync --daemon 加到 /etc/rc.local 檔案中，系統開機時即自動 啟動；亦可在系統提示符號下，下達指令：

```
# rsync --daemon
```

3. 設定 /etc/rsyncd.conf

```
[ylc]
path            = /home/data
comment         = ccu www project
max connections = 20
read only       = true
hosts allow     = 163.27.0.0/16
hosts deny      = *.*.*.*
lock file       = /tmp/rsyncd0.lock
```

4. 設定密碼檔:

直接在 rsyncd.secrets 設定帳號:密碼，如：

```
ylc:AutoUpdate
```

接著必須將 rsyncd.secrets 密碼檔的檔案屬性設為 root 擁有，且權限要設為 600，否則無法備份成功，命令:

```
chown root.root rsyncd.secrets
chmod 600 rsyncd.secrets
```

3-3 區域網路中心及縣市教育網路中心

為避免網路頻寬不必要的浪費，同時也避免不當資訊防制死角的出現，因此，在區域網路中心及縣市教育網路中心則採用透通式代理伺服器架構，也就是利用網路骨幹設備的 WCCP 功能強制將 HTTP request 重新導向 Proxy Server，一方面可以透過代理伺服器的快取 (caching) 功能，減少網路上的 HTTP request 流量，同時也縮短使用者等待回應的時間；當使用者均能透過 Proxy Server 存取網頁時，對於舒解網路壅塞的情況亦有相當大的幫助，也使得整體的網路服務品質大幅提高，而代理伺服器亦可更快速擷取到使用者需要的網頁內容，因此也有助於縮短使用者等待回應的時間。

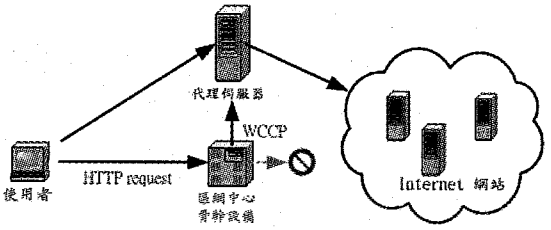

圖 8 透通式代理伺服器架構示意圖

3-4 下游學校

由於本研究利用網路從眾行為的理論為基礎，建立一份以瀏覽次數排序過的不當資訊清單，下游學校只需瀏覽次數排名較前面的一小份清單即可達到最大的過濾攔阻效果，而不需要把整個不當資訊清單的 10 萬餘筆記錄全都加到攔阻清單，因此，對於系統效能的影響相當小，如果只擷取其前面幾百筆的記錄，對系統負荷幾乎不會造成多少影響。因此，下游學校可以不用額外增購電腦主機，只需用現有的電腦即可配合，因此不會造成成本的增加。下游學校只要安裝 rsync 指令，並完成下列工作:

1. 設定密碼檔

密碼檔放在 /root/rsyncd.secrets, 內容只要含有密碼一行即可:

```
AutoUpdate
```

2. 利用 crontab 自動排程，於每週進行更新。

```
0 2 * * 7 /root/squidGuard.update
```

3. 重新啟動 squidGuard 使其生效，程式如下：

```
#!/bin/csh
set SquidGuard=/var/db/squidGuard/SquidGuard
set WWWSquidGuard=/home/www/data/SquidGuard
set masterHost=163.27.nnn.nnn
set masterDir=SquidGuard
rsync -av --stats rsync://$masterHost/$masterDir/
$SquidGuard/
rsync -av --stats rsync://$masterHost/$masterDir/
$WWWSquidGuard/
```

```
chown -R nobody:nogroup $SquidGuard
squidGuard -c /usr/local/squid/etc/squidGuard.conf -d
-C all
/usr/local/squid/bin/squid -k reconfigure
```

3-5 落實的關鍵因素

就以往的實務經驗而言，過多不當資訊黑名單的資料筆數對許多下游學校的設備而言，會造成其系統的嚴重負荷，甚至導至系統當機，最後不得不停止不當資訊的攔阻；此外，有許多下游學校沒有專職的資訊人員，這也是導致下游學校配合意願較低的主因，因此，要達成本研究所提出的區域聯防體系，主要的關鍵有下列兩點：

1. 不當資訊黑名單的完善與否是此一架構的主要成敗因素，此一黑名單資料庫必須：
   a. 能夠有效降低記錄筆數以供下游學校單位使用，才不致於造成下游學校的主機負荷加重，此一機制才得以持續運作。
   b. 能夠動態而有效的新增不當資訊清單，以配合攔阻目前危害較高的熱門不當資訊網站。
   c. 必須能夠剔除資料庫中已經不存在的不當資訊網站的記錄，以免此資料庫不斷的增長且不符合現況。
2. 自動化機制的建立以避免造成人力上負擔，主要包括：
   a. 在區域網路中心方面，如何自動化新增及剔除不當資訊清單的網站，以得到最大的攔阻效果。
   b. 在區網中心和眾多下游學校間如何建立有效的自動化傳輸機制，使下游學校可以取得最新的不當資訊攔阻清單。
   c. 在下游學校方面，如何自動更新 squidGuard 不當資訊清單資料庫，以發揮最大的功效。

4.實作結果分析

為確定本研究所建立的不當資訊清單是否具有預期的從眾行為，我們收集了雲嘉區域網路中心及所屬教育網路中心四月份所有 Proxy Server 的記錄檔總共計5億9千萬多筆記錄，進行比對及統計，結果發現共有 1,934 個不當資訊網站曾經被瀏覽，request 總數為 36,816,986，且使用者在瀏覽不當資訊網站時有明顯的從眾行為，經統計（如表 1，圖 9）後發現，若以瀏覽次數最高的前一百名熱門網站作為攔阻對象，其攔阻率可以達到 73%，若增加為前二百名，則攔阻可達 85%；依序增加到前五百名，則攔阻率已可高達 95%。

表 1 不當資訊瀏覽分析表

瀏覽排行	Request 次數	百分比
Top 100	26,962,077	73%
Top 200	31,159,031	85%
Top 300	33,038,028	90%
Top 400	34,162,086	93%
Top 500	34,898,394	95%
Top 600	35,420,169	96%
Top 700	35,807,557	97%
Top 800	36,082,347	98%
Top 900	36,282,056	99%
Top 1000	36,423,197	99%
Top 1100	36,532,261	99%
Top 1200	36,620,754	99%
Top 1300	36,686,584	100%
:	:	100%

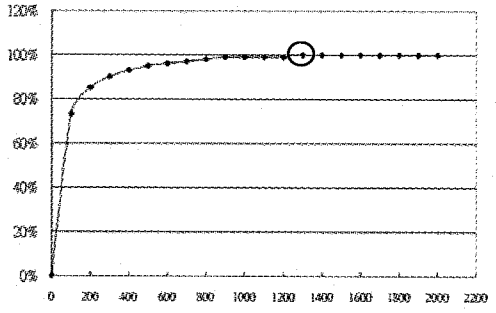

圖 9 Top n 命中率統計圖

5. 結論

由上面的圖表，我們可以發現到不當資訊的瀏覽行為的確具有非常明顯的從眾性，因此，我們可以利用此一清單有效減少過濾攔組的記錄筆數，下游學校只需要以 1,300 筆不當資訊黑名單就可以過濾掉 99% 以上的不當資訊，若下游學校的機器效能不佳，覺得系統負荷較重，亦可視情況減少不當資訊黑名單的筆數，亦能達到相當好的效果。

由於本研究所提出的架構主要是透過下游學校進行第一線的攔阻，因此，在下游學校能夠有效的攔阻掉絕大多數不當資 request 的情況下，對於上游單位的不當資訊防制設備及代理伺服器的負荷將可以大幅降低，因此，對於網路的服務品質也將可以大幅提昇，這對於使用者和管理者而言，無疑都是雙贏的結果。

參考文獻

1. N2H2 Inc., "Reports Number of Pornographic Web Pages Now Tops 260 Million and Growing at an Unprecedented Rate", 2004, http://www.n2h2.com/
2. Reuters, "Web Porn Entices Far More Surfers Than Search-Study", 2004, http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=5340076
3. 教育部，民92，「TANet不當資訊防制計畫」，http://www.edu.tw/moecc/index.htm。
4. Mowen, J. C. and Minor, M. ,"Consumer Behavior," 5th ed., New Jersey: Prentice-Hall, Inc., pp.487-489, 1998.
5. Asch, S. E. "Effect of Group Pressure Upon the Modification and Distortion of Judgments," Journal of Marketing Research, 16, pp.394-400, 1951.
6. Asch, S. E. Social Psychology, New York:Prentice-hall,1952.
7. Asch, S. E. "Studies of Independence and Conformity: A Majority of One Against a Unamimous Majority," Psychological Monographs, pp.70-79, 1956.
8. Hanson, W., and Putler D. "Hits and Misses: Herd Behavior and Online Product Popularity," Marketing Letters (7:4), pp.297-305, 1996.
9. Malatesta, G. "Conformity Rules in Cyberspace," 2001, http://www.theaustralian.news.com.au/printpage/0,5942,2651185,00.html.