網路匯集點的 P2P 訊務量測
Flow-based P2P Traffic Measurement

楊素秋　曾黎明
中央大學 電子計算機中心　資訊工程系
center7@cc.ncu.edu.tw　tsenglm@cc.ncu.edu.tw

摘要

隨著寬頻 Internet 網路的普及電腦硬碟容量的大幅提升,網路用戶很自然地藉由高效率的分散式 P2P 檔案軟體交換 VCD 或 DVD 的影片或歌曲, 造成 Internet 訊務的嚴重失衡:少數 P2P 用戶的訊務耗盡連線頻寬,影響大部分使用者的權益,及帶來頻繁的網路財產侵權的抱怨.

由於 P2P 軟體已完全打破傳統主從的(Client /Server) 傳輸模式.不僅將檔案切割成多個 fragments,將資源分散儲存在各個 participate peer 系統,也允許 peer 選取任意 socket port number (0 ~ 65535 間之任意整數) 與 peers 建立傳輸連結,快速抓取部分內容,再結合成完整檔案.這些 P2P 特有的傳訊策略都使得網路管理者無法再依據特定傳輸 port 辨識/累計 P2P 訊務.

TANET 區網 Aggregate router 座於連網閘門位置, 負責轉送該地理分區大學,高中職,及數百所國中小學的 Internet 輸出/入訊務.本研究擬擷取 router NetFlow data,利用精簡的 NetFlow 轉送紀錄, 實地追蹤與分析 P2P socket 傳訊特徵,系統並依據 P2P 的並行傳輸特性,選定適當的傳訊特徵, 讀取 NetFlow data 累計/排序相關訊務數值,再據以偵測轉送的 P2P 訊務,協助管理人員監看其具體 P2P 傳訊量, 找出 P2P 主機,甚至寄發網路著作財產權宣導資料給可能的 P2P 用戶.

Abstract

P2P technology not only removes central control of such resources as communication, computation, file storage and retrieval, current P2P applications also have the ability to use arbitrary ports to camouflage their existence. The participants in the system thus could easily hide personal identifying information easily.

As P2P traffic can not be classified by simply looking at the IP packet headers, This work makes use of the NetFlow data export from a aggregate router to develop P2P traffic measurement that helps identify active P2P stubs according to its significant distribution features: (1) heavy connection density, (2) large mean packet size, and (3) long transmission duration.

關鍵字: P2P, traffic measurement, intelligent property.

1. 研究動機

隨著寬頻 Internet 的普及電腦硬碟容量的大幅提升, 網路用戶很自然地在自己 PC 儲存大量的應用軟體,音樂/影片,藉由分散式的 P2P (Peer-to-Peer)軟體與廣大網路用戶交換 VCD 或 DVD 影片/歌曲, 造成 Internet Elephant and mouse 的兩極化應用分野. 急速成長的 P2P 影音交換訊務的轉送成為 ISP (Inernet Service Providers)的最大挑戰:少數 P2P 用戶耗盡網路頻寬,影響大部分使用者的權益.

除了佔用 ISP 連網頻寬, P2P 影音交換訊務也帶來頻繁的網路著作侵權抱怨. 網路用戶雖知道: 透過 P2P 軟体搜尋/下載的影音檔案(包括: 影片, 商用軟體, MP3 音樂)往往是受到著作權保護的,雖擔心會因違反智慧財產權法而受到處罰,卻又超想要免費的檔案. 結果往往是:矛盾地選擇啟動 P2P 交換軟體,擷取"超想要的檔案", 結果是:一封又一封的智財權抱怨信件.

欲導正網路用戶對智財權的尊重, 改善網路效能與著作侵權問題, 亟需就該網路轉送的 P2P 訊務做量測,協助管理者掌握具體的 Top-N P2P 輸出入訊務,據以寄發網路著作財產權宣

導資料甚至適度限頻超量的 P2P 傳訊流.

本文於第二節敘述相關的 P2P 訊務量測研究. 第三節分析熱門 P2P 應用傳訊特徵. 第四節陳述實做的 P2P 訊務監測系統, 包括: P2P stub 的辨識, 訊務與持續傳輸時段的累計, 分析監測的單日 P2P 訊務數據. 最後於第五節做成結論.

2. 相關研究

P2P 交換軟體完全突破傳統主從式(Client /Server) 傳輸模式, 將系統及網路資源分散在各個 peer 系統, 除了將檔案切割成多個 fragments 儲存, 使單一個檔案可以由多個 peers 同時抓取, 提高傳檔速率外; 大部分 P2P 軟體也允許使用者選取任意 socket port number, 與多個 peers 同時建立傳輸連結, 交換影音訊務, 這種特有的傳訊策略使得網路管理者無法再依據特定的傳輸 port number 辨識/累計 P2P 訊務.

Tutschku K.[1] 曾分析監聽自校園一 FastEthernet 主幹的封包內容, 分析使用 4662/TCP 的 eDonkey P2P flow 與一般 Internet 應用 flow 的差異. 研究結果顯示: eDonkey 連接的**傳輸訊務容量 (flow size)** 數百倍一般應用. 而 download flow **連接的持續傳輸時間(TCP hold time)**也為一般應用 flow 傳輸時間的數百倍.

Karagiannis T. 等人[2] 利用監聽自一 OC48 (2.5Gbps) 主幹的封包(header & content), 再依據下列三個程序辨識 P2P flows, (i) port number 落在 well-know P2P port list 者, Flag 為 P2P 應用, (ii) 若未使用 well-know P2P port 者,進而比對 16-bytes 的 payload 特殊字元, 若比對成功則 Flag 為 P2P 應用,若比對失敗則 Flag 為 non-P2P 應用, (iii) 將前兩步驟成功 flag 的 IP 位址加入 P2P_IP hash table; 視為"possible P2P". 其研究結果顯示: 當時該演算法能正確辨識 95%的 P2P flows. False positive 為 8 %~ 12 %.

Wagner A.等人[3] 則僅依據 well-known P2P port 的比對辨識 P2P flows, (i) local IP hosts 的 port number 若落在 well-know P2P port list, Flag 為 P2P 應用, (ii) 若與 local IP hosts 建立連接 IP 的 port number 為 well-know P2P port 則 Flag 為 non-P2P 應用. (iii) 每隔固定時段,顯示 active P2P peer {IP,Port}及傳送的訊務總量.

Yang [4] 監聽一條 GigaEthernet 主幹網路的封包內容, 依據 GNUTELLA, eDonket, BitTorrent 的連線特殊字串,找出 P2P stub, {IP address, port}, 累計 P2P stub 的傳訊量及判別採用的 P2P 應用程式種類.

3. P2P 傳訊特性

為提供網路管理人員較詳細的 P2P 訊務統計資訊,本研究先探討熱門 P2P 傳輸應用軟體的傳輸特性, 實地追蹤/分析/歸納 P2P flow 的傳輸特徵,作為 Feature-based P2P 訊務累計傳訊數據的基礎.

3.1 熱門的 P2P 應用軟體

3.1.1 GNUTELLA

為有效找尋與轉送檔案/資料, GNUTELLA 除了採用類似 HTTP 的商議協定提供基本連接資訊的交換與維護功能外, 也使用雙向的 TCP streaming, 提供可靠的 P2P 通訊, 並增加適當的 bandwidth 管理機制, 避免壅塞用戶實體連線訊務[5].

3.1.2 eDonkey/eMule

eDonkey 採 hybrid P2P 傳輸架構 [2], (A) 透過 index server 協助找尋與其建有連接的 P2P 主機. peer 一旦開始 search file, 會先要求與 main index server 建立連接, 待 main server 回傳 matched 的檔案及位置後. 才再次要求與其他 index server 建立連接, 找出其他 matched 的檔案及位置.

其後, Client 開始檔案的下載程序. 向存有 matched list 的 peers 要求一 upload queue. 待 providing client 將要求置入其 upload queue, 並發現滿足其預設頻寬限值時, 會要求與 request peer 建立連接/傳輸檔案. 預設的 eDonket 傳輸 port 為 4662/tcp, 但允許用戶選定任意 port 建立連接.

eMule 為 eDonkey 的擴充版 [6], eMule peer 預設有多個 index servers, peer 藉由這些 index server 進入 P2P 網路. Peer 除了維持一 upload queue 以分享其既有檔案. 當 Download 的連接要求被置入這些 upload queue 底部, 並被排程到 queue 上端時, 才開始檔案傳輸.

3.1.3 BitTorrent (BT)

BitToorent 採用 tracker 程式, 透過 HTTP 協定交換下載檔案資訊, 包括: download 檔案

名稱, link 的 port, peers 的聯繫資訊等. 此外,也藉由 credit 評量及 choking 演算法, 提供高效率,強建,公平的 P2P 檔案分享[7]. 透過簡單使用介面: 使用者只要 click 欲 download 檔案對應的 hyperlink,給定對應的儲存名稱,即開始下載檔案.

3.2 P2P 傳訊特性

Router NetFlow 係將轉送封包 header 的基本 flow 資訊做簡單加總後,定時 export 給蒐集的 client 系統,提供作 trouble shooting, top-N user list, 或 billing 用途. NetFlow 將典型的雙向(bi-direction) TCP 傳輸加總後紀錄為兩筆單向的傳輸紀錄: 其一紀錄 source 連接至 destination 的訊務變量,另一則表示由 destination 連接至 source 的傳訊量.

藉由區網 router NetFlow data 追蹤典型的 eDonkey P2P stub (IP_Addr/4662 port),可以輕易歸納明顯的 P2P 傳輸特徵: peer **主機依據用戶選定 port number,同時與成群的 peer 建立連接,傳送大封包的訊務** (圖 3.1). 因此, 本研究選擇 IP 位址與應用埠(port), 2 項 NetFlow 訊務變量作為 virtual flow,並限制 Feature-based 訊務累計程式加總/辨識出同時開啟多個 process,與多個 peers 建立連接,傳輸近乎滿封包的 stub 訊務.

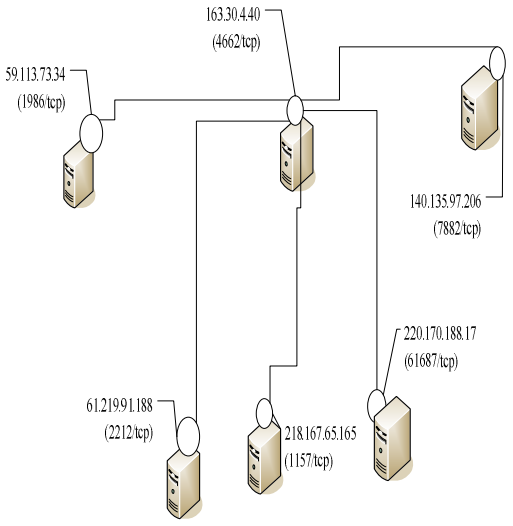

圖 3.1 P2P 通訊概要模式

4. Flow-based P2P 訊務量測

Flow-based P2P 訊務量測系統包含三個功能模塊: (A) Active P2P stub 辨識程式,(B) P2P 訊務累計程式,與(C)P2P 訊務偵測程式.

4.1 P2P 訊務累計程序

首先, 辨識程式持續讀入每 10 分鐘儲存的 Netflow data 檔, 將 source IP, destination IP 與所選定的 local IP 位址比對 (例如:該主幹轉送 **140.135.**0.0 校園訊務),分辨 輸出或輸入 flow 連接.再累計並排序傳送大封包 peer stubs (例如: **140.135.**152.71:12998) 的連接總數,訊務量,計算平均封包大小,並依 flow 連接數量大小排序, 儲存到對應於各時段的輸入/輸出訊務檔.

其次, P2P 訊務累計程式讀入先前累計的各時段的輸入/輸出訊務檔,累計連接超頻繁 P2P stub 的訊務變量.最後,偵測程式再據以加總每一 stub 的 flow 數,packet 數, byte 數,與 mean packet size 訊務變量, 比對多個訊務變量臨界值,突顯每小時的 P2P stub 及其具體傳訊數據.

最後, P2P 訊務偵測程式讀入各時段累計的訊務變量,加總 stub 建立的 flow 總數 (flow[$stub_i$]), 所送出的封包總量 (packet[$stub_i$]),訊務總量(byte[$stub_i$]),與平均封包大小(pkt_size[$stub_i$]) 等變量.再加總其持續時段(duration[$stub_i$] ,推計其每小時建立的平均連接數 (flow_rate[$stub_i$]. 最後,程式將各變量與估定臨界值比對,找出持續/快速轉送鉅量 content 的 P2P stubs 儲存檔案.

4.2 P2P 訊務監測網頁

依據偵測的 P2P 具體訊務數據,管理人員能有效地與使用者溝通/解釋其系統的問題,掌握: 哪些源端主機,送出超大量 P2P 訊務變量 (Octets, packets, mean_packet_size).

圖 4.1 所示為單日的 P2P Host 輸入/輸出訊務監測網頁,網路管理者可監看其連線承載的 Top-N P2P 用戶資訊,包括: 網路主機的 IP 位址, 輸入訊務量, 輸出訊務量,總訊務量, 及傳訊持續狀況.掌握更詳細 P2P socket stub 的訊務資訊.

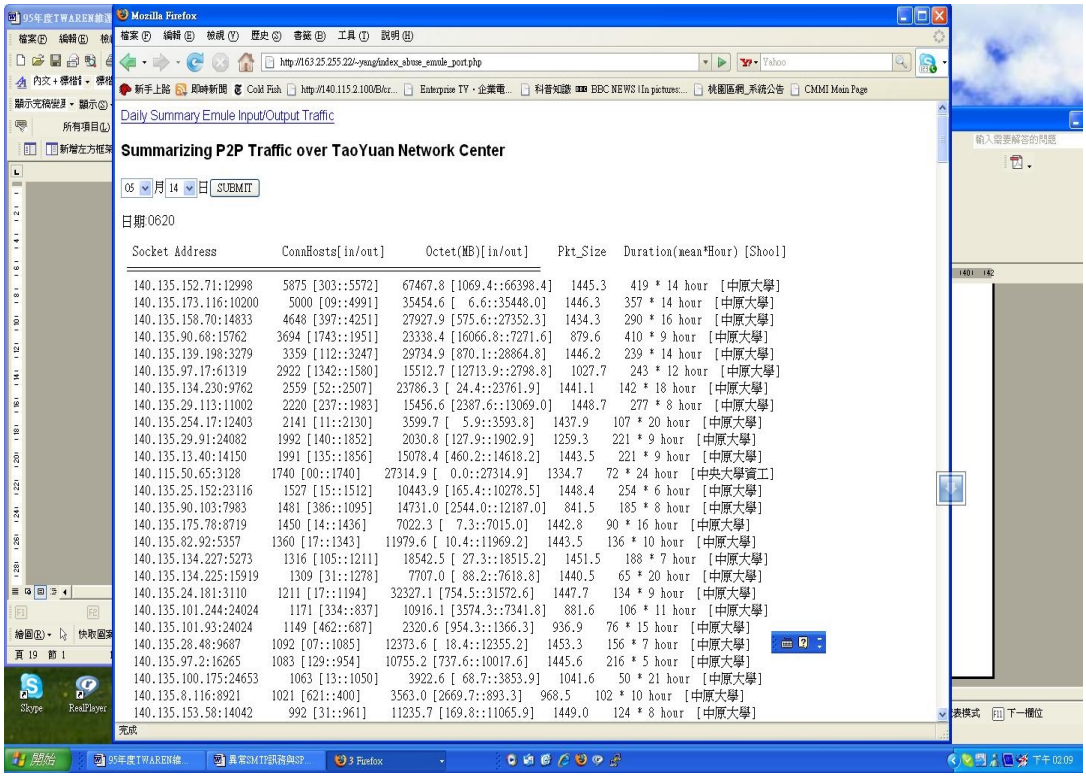

圖 4.1 Top-N P2P Stubs 訊務監測網頁

5. 結語

迅速成長的 P2P 超大容量視音訊檔案交換,除了快速耗盡連網頻寬外,也導致頻仍的智慧財產侵權抱怨. 網路管理單位非常需要實做精確的 P2P 訊務量測,協助管理人員掌握,甚至制定適當管理策略, 適度限頻P2P 訊務流,維持應有的網路傳輸效能.

本研究擷取區網匯集 router 送出的 NetFlow data,利用精簡的轉送紀錄(非 packet content), 實地追蹤與分析 P2P socket 傳訊特徵,依據P2P 的多項傳訊特徵,萃取/累計得單日之 P2P 訊務,協助網管人員監看,寄發網路著作財產權宣導資料.

該系統已成功地架設於 TANet 區網中心,協助管理者監看/發現 P2P 大戶的主機 IP, port number. **依據連線學校網管實地訪查所偵測P2P 用戶的回應狀況,也是相當正面的.** 未來,我們會嘗試運用網路封包內容的交互比對或 data mining 方法,更精確/快速地偵測 P2P 訊務,以自動寄發智財權宣導文件,或配合適當的限流策略,維持應有的網路效能

參考文獻

1. Tutschku K., **A Measurement-based Traffic Profile of the eDonkey Filesharing Service**, The 5th annual Passive & Active Measurement Workshop, April 2004, pages 12–21.
2. Karagiannis T., Broido A., Faloutsos M., and Claffy K, **Transport layer identification of P2P traffic,** Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, 2004, Pages: 121 - 134.
3. Wagner A., Dubendorfer T., Hammerle L., Plattner B., **Identifying P2P Heavy-Hitters from Network**, the Second Annual FloCon Workshop, 2005.
4. 楊素秋, 曾黎明, 以封包內容為基礎的 P2P 訊務監測系統, TANET2006 論文集.
5. **Gnutella2 Specification Document**, www.mousearmy.net/tech/gnutella2.pdf.
6. Kulbak Y., Bickson D., **The eMule Protocol Specification**, http://www.cs.huji.ac.il/labs/danss/presentations/emule.pdf.
7. Cohen B., **Incentive build Robustness in BitTorrent**, http://www.bittorrent.com/bittorrentecon.pdf, May 2003.