SONET 網路傳訊品質與 UDP/ICMP 訊務的迴歸相關分析

楊素秋　曾黎明
國立中央大學 電算中心 資訊工程學系
Email: center7@cc.ncu.edu.tw (corresponding author)

摘　要

隨著國外訊務的迅速成長, TANet 國外連網訊務也迅達飽和使用狀態, 為統計大量國外訊務對 OC3 Sonet medium 傳輸品質的影響. 本研究擷取國外傳訊 router 的 Netflow 訊務轉送 log,及 Sonet 傳訊 MIB.統計連線承載的 TCP/UDP/ICMP 訊務量分布,及對應的 medium 傳輸 Coding Violation (CV)頻次分布,計算 Sonet CV 頻次與所承載 UDP/ICMP competition 訊務的迴歸相關.統計數據顯示:國外連網尖峰時段出現的明顯 TCP traffic degression 與持續的 ICMP burst 訊務明顯相關. 而 UDP,ICMP 訊務則均與尖峰時段的 Sonet CV burst 明顯相關.

[註] 本論文接受教育部電子計算機中心的委託與補助.(編號 91078067)

1. 引言

Internet 連網的開放特性不僅造就了多元的網路應用型態,結合 Data 與 real time Streaming Media 傳訊則更加速連網訊務的成長,帶來網路壅塞與傳輸品質劣化的問題. TANet 國外連線為國內學術研究機構連上國際網路的最主要途徑, 為掌握 competitive UDP/ICMP 訊務與其 Sonet 傳訊品質的相關. 本研究擷取 WAN route Sonet medium 傳訊 MIB 與 light-weight 的 router 轉送訊務 log,實做 medium 傳輸 Coding Violation (CV)頻次與承載非自律訊務的量測,並藉由具體的訊務數據分析競爭性應用訊務與 Sonet medium 傳輸品質的相關.

1.1 Sonet 傳輸

Synchronous Optical Network (SONET)光纖網路標準定義的傳輸速率(Rate)及 Frame,除了提供同步切換(synchronous multiplexing)多個 signal 傳輸 blocks 的格式外,也制定彈性組合多種寬頻傳輸速率的標準[1]. 藉由 4 個光纖界接層界接 Synchronous Transport Signal (STS) format 與 user 端點設備 format 的轉換. path layer map 多個 end device signals 成為符合 line layer 需求的 Sonet format. line layer 處理傳輸資料的同步與 path layer block 的多工切割/組合.section layer 則處理 physical medium 傳輸的 Framing, Scrambling, Error monitoring,及 Section Maintenance.

除了 Section overhead (SOH)依據 Framing 紀錄的 Out Of Frame (OOF)錯誤紀錄外, Path/ Line/ Section 封包的 Bit Interleaved Parity (BIP) OverHead 均累計對應各層傳輸錯誤的 MIB Counters, 包括:傳輸的 Code Violations (CV), 累計出現的 BIP 傳輸錯誤或 Out of framing 錯誤次數. Error Seconds (ES) 累計曾發生 CV 或 Loss of Signal (LOS) 的秒數, Severely Error Seconds (SES)累計曾發生多於 CV threshold 值錯誤的秒數. UnAvailable Seconds (UAS)累計完全無法使用連線 Medium 的秒數. 此外,SNMP Agent 也累計各 Sonet layer 最近的

96 個 per-15-min interval Sonet MIB [2], 包括: SectionInterval, LineInterval, FarEndLineInterval, PathInterval, FarEndPathInterval 的 CV, **E**S,UAS MIB;藉由 routine 的 SNMP pooling 即可蒐集 OC3 連線 CV MIB,提供長期 Sonet Link 傳訊品質的統計與分析.

1.2 相關研究

藉由網路傳輸封包 herder 的監聽,網管人員始得以依據 end-to-end 的 IP address,length, 及 TCP/UDP application ports,統計與分析連網的確切運務量與訊務特性. Barnet B.G. [3] 曾藉由 Tcpdump 監聽區域網段傳送的封包 headers, 重複訊務 logs 的 parsing 與加總處理, 統計 NFS UDP, UDP, TCP, Decnet 等區域網路協定的訊務分布. Kushida T. [4] 也曾透過 Tcpdump 監聽 FDDI 網段 packet log, 量測其研究網路的 TCP, UDP 訊務量與傳訊特性. Thompson K. 則利用 MCI OC3MON 軟/硬體量測 ATM 連線承載的 TCP 與 UDP 訊務及熱門應用訊務分布 [5].

由於 WAN router 轉送所有的 Internet 訊務, router 得以高效率地暫存/加總每一過境封包的 header 資訊,週期性地將轉送 flow 資訊送與蒐集的 UNIX PC 主機. PC 僅需透過 flow-tools shareware 的執行, 接收與儲存 router 的 Netflow 訊務紀錄[7],進行 light-weight 的訊務特性分析. Flow-based 的訊務 log 紀錄包括: TCP/UDP/ICMP protocol identification, source IP address, source port, destination IP address, destination port, source routing interface, destination routing interface, packet count, 及 byte count. 本研究則比對 flow 的 source /destination interface 及 protocol identification 紀錄的比對,統計 TANet 連接 U.S.Internet 的 Sonet OC3 連線 TCP/UDP/ICMP 輸入/輸出訊務量.

本文將於第二節分析 SNMP (Simple Network Management Protocol Get) pooling 蒐集的國外連線 Sonet UAS 與 CV 頻次. 第三節分析藉由連網 router Netflow 訊務轉送 log,統計的 TCP/UDP/ICMP 訊務分布. 第四節分析 Sonet CV 傳訊錯誤變量與 UDP/ICMP 訊務變量的迴歸相關. 最後於第五節做成結論.

2. Sonet 光纖傳輸品質的監測

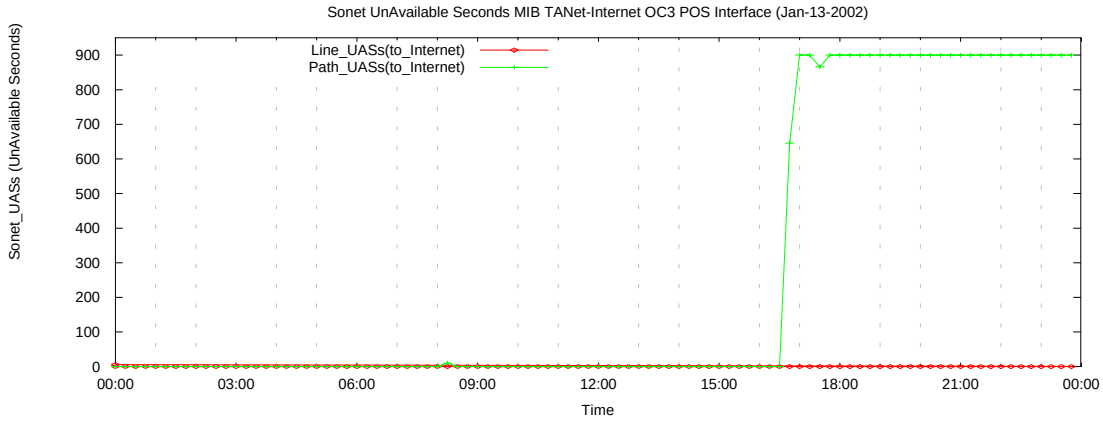
本節將分析 TANet 國外連網 router OC3 介面的 Sonet 傳輸層的 CV 頻次,甚至嚴重的 UAS 傳輸錯誤分布.

2.1 OC3 Sonet MIB 的量測

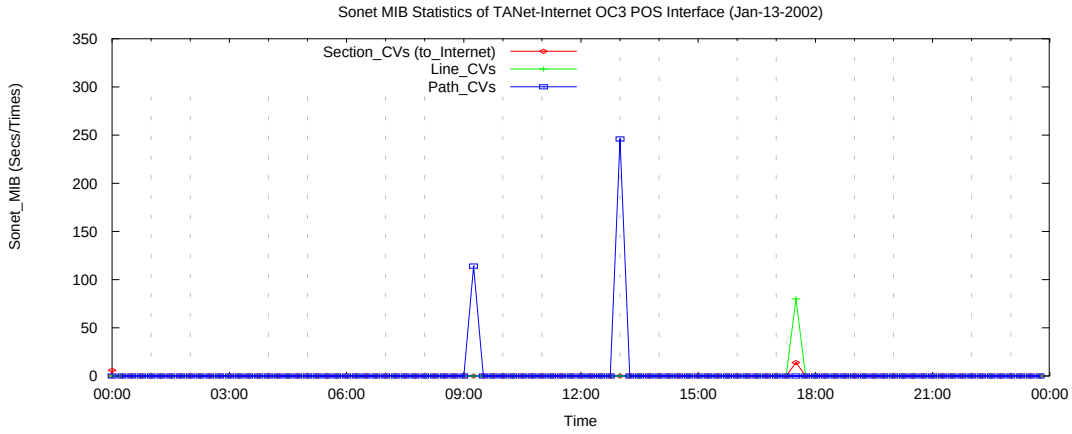
SNMP 協定定義網路設備間管理資訊的交換管道, Sonet 光纖傳輸 MIB Schema 的訂定則允許網路設備實現 SNMP agent [8], 允許網管人員應用 snmpget 程式擷取/分析網路設備的各層訊務 MIB.透過 cron 定期 pooling 的 SNMP MIB 則有助於 Sonet Link CV, **E**S, UAS 等傳訊品質參數的長期追蹤.

Fig. 1 顯示 TANet-Internet OC3 Sonet 介面中斷時實測的 ES, CV, UAS 傳輸錯誤頻次分布(Jan-13-2002). 對應於 17:00~23:59 訊務中斷期間的 per-15-min Path UASs 值均為最高的 900 秒. 也可明顯發現 9:00 及 13:00 訊務尖峰出現的高 Path CVs 值 (Fig.1b). Fig. 2 顯示一般工作日的國外 OC3 Sonet MIB 分布 (Mar-06-2002, Wednesday). 連網雖未出現嚴重 ES 及 UAS 錯誤,但仍可發現明顯的 Sonet CVs 發生於 15:00~21:00 訊務尖峰時段.下一節將進而統計國外連網承載的 TCP/UDP/ICMP 訊務,

分析 Sonet CV 傳輸錯誤頻次與對應 UDP/ICMP burst 訊務的相關.

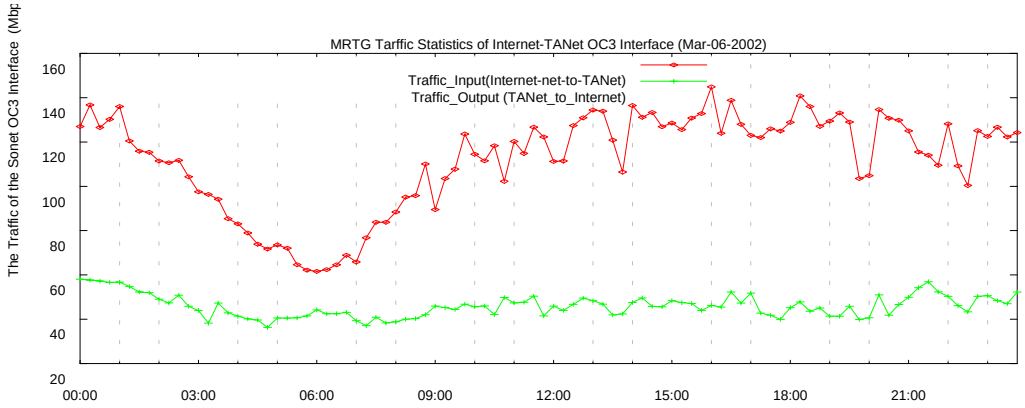


(a) The Sonet Line/Path UnAvailable Seconds (UAS) Plots

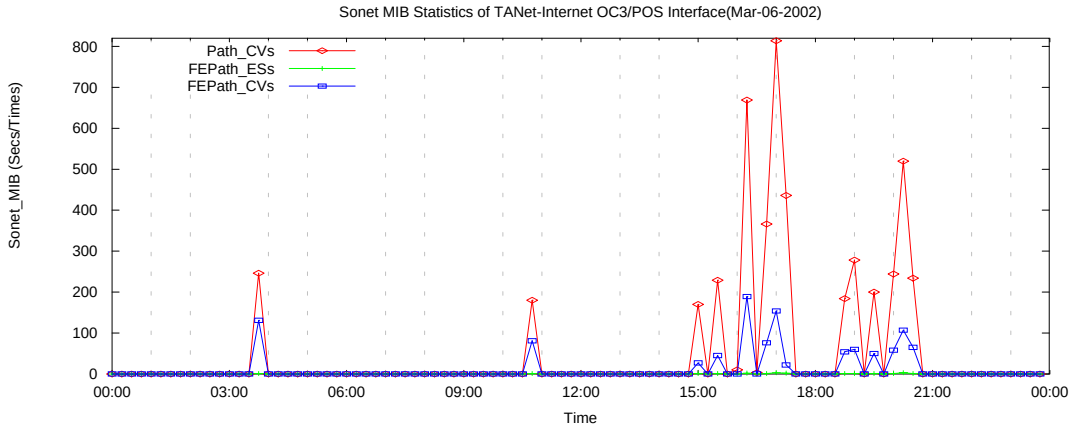


(b) The Sonet Coding Violation Plots

Fig. 1. The Sonet_UAS/CV Statistics of TANet-Internet Sonet Link



(a) The Traffic Plots of the Sonet Interface



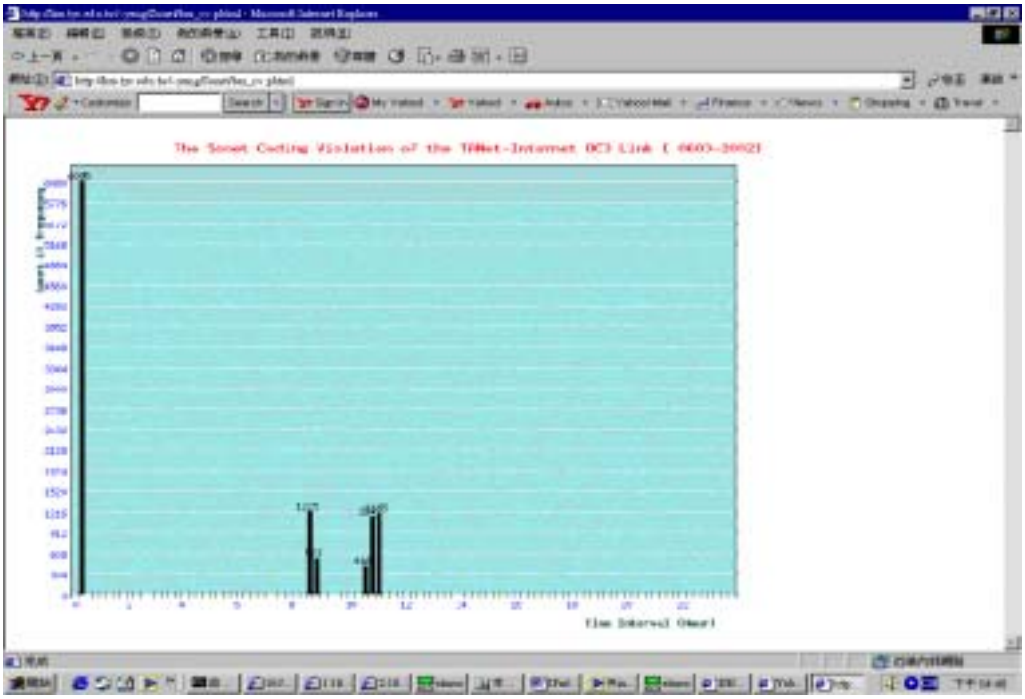
(b) Sonet Coding Violation (CV) Statistics

Fig. 2. The Coding Violation Statistics of TANet-Internt OC3 Sonet Link

2.2. Sonet 傳輸品質監測網頁

Hypertext Preprocessor (PHP)是一種使用相當普及的 scripting 程式語言, 常被內嵌於 HTML 檔用以製作 Web 動態網頁. 為提供用戶能隨時監測國外 Sonet 傳訊品質, 我們首先安裝 apache (WWW) server , Graphic (GD) 圖像程式庫及 PHP 程式語言 [9] [10]. 再撰寫程式: 讀取 snmp pulling 取的的 Sonet MIB 存檔,並呼叫 PHP 的圖像函數,動態生成 Sonet CV 傳輸錯誤頻次的圖像數輸出到監測網頁. 於用戶輸入查詢日期後, invoke PHP 程式讀取 CV 數據,將對應日期的連網 Path CV 分布顯示於網頁(Fig.3).

(a) 日期輸入網頁



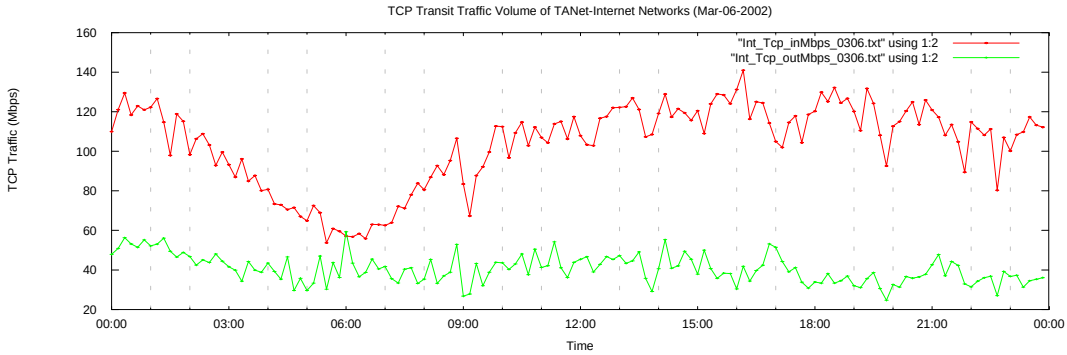
(b) Sonet Path CV 傳訊品質監測網頁

Fig. 3. The Daily Path CV Statistics of TANet-Internet Sonet Link

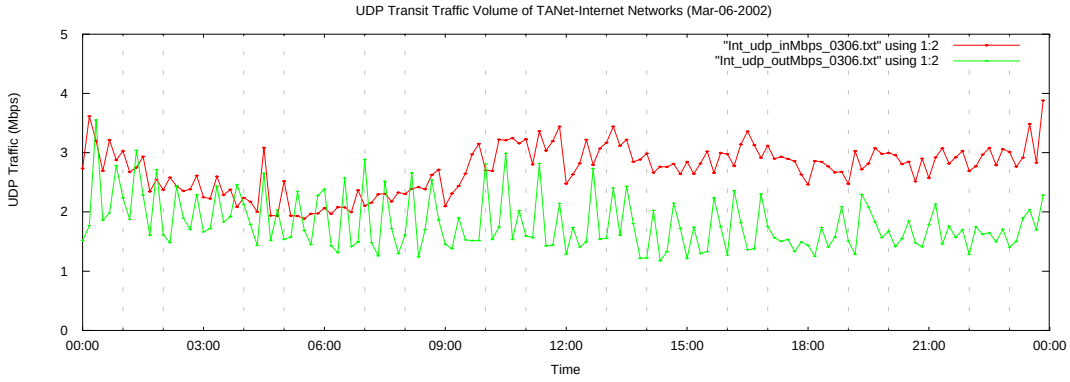
3. TCP/UDP/ICMP 訊務的量測

為分析國外 Sonet 連線承載的 TCP/UDP/ICMP 訊務, 我們利用 collecting host 蒐集的 per-10-min netflow traffic log. 比對 source/destination interface 及 protocol identifier, 辨識 TCP, UDP 及 ICMP 封包,並分別累計到對應 $flow_i$ 的 per-10-min TCP/UDP/ICMP 訊務變量: $flow_i$.in_tcp, $flow_i$.out_tcp, $flow_i$.in_udp, $flow_i$.out_udp, $flow_i$.in_icmp, $flow_i$.out_icmp, 統計 OC3 link 承載的單日 per-10-min TCP/UDP/ICMP 輸出入訊務分布.

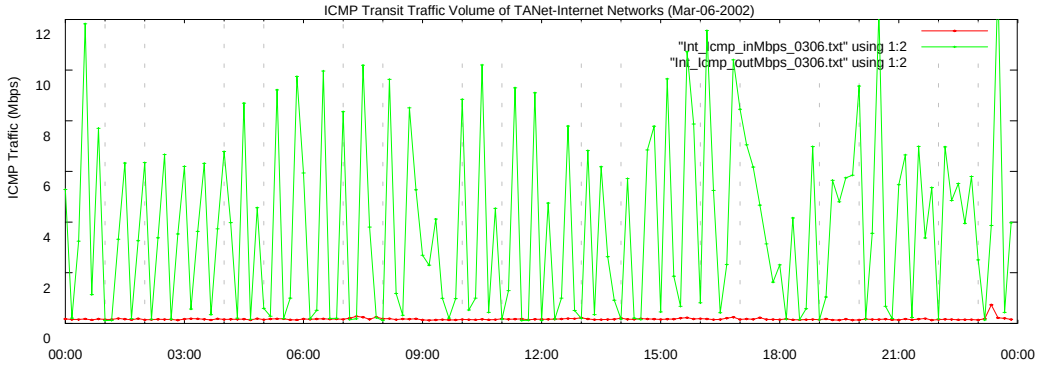
Fig.4(a) 顯示統計的 TANet-Internet OC3 Link TCP 訊務量分布圖(Mar-06-2002). 國外輸入到 TANet 的 Input TCP 訊務明顯高於 Output 訊務. TCP 訊務高峰自上班時段續到深夜, TCP Input 訊務速率約為 110 Mbps, TCP Output 訊務速率接近於 40 Mbps.明顯的 TCP traffic degression 出現於 1:30, 9:00, 17:00, 19:30, 22:00, 22:30 等時段.相較之下, OC3 Link 承載的 UDP 訊務分布較 TCP 訊務平均. 而該日輸出到國外的 ICMP burst 訊務也明顯偏高 (Fig.4c),明顯 ICMP 持續訊務分布於: 0:30-1:00, 8:30-9:30, 16:30-17:30, 19:00-20:00, 21:30-23:00 時段,則大致對應於 TCP Traffic Degression 時段.



(a) Daily TCP Traffic Statistics



(b) Daily UDP Traffic Statistics



(c) Daily ICMP Traffic Statistics

Fig. 4. The TCP/UDP/ICMP Traffic Statistics of TANet-Internt OC3 Link

4. UDP/ICMP 訊務與傳訊品質的相關

4.1 UDP/ICMP 訊務與 TCP Traffic Degression 的相關

由於 TANet 輸出往國外的 ICMP burst 平均的傳訊速率偏高,最高值近乎 10 Mbps; 我們繼而統計國外 TCP Traffic Degression 與 UDP/ICMP 訊務的相關, 本節利用統計得的 TCP/UDP/ICMP 訊務數據, 分別取樣每 6 個時間單元的 UDP_i,$ICMP_i$,與 (Max_BW – TCP_i) 訊務變量, 帶入兩變數 X, Y 樣本相關係數 r (sample correlation coefficient)計算式 [11],計算單日各 time interval UDP/ICMP 與 TCP Degression 訊務變量間的迴歸相關係數分布.

$$r_i = \frac{(S_{xy})_i}{\sqrt{(S_{xx})_i (S_{yy})_i}} \quad \text{----- (1),}$$

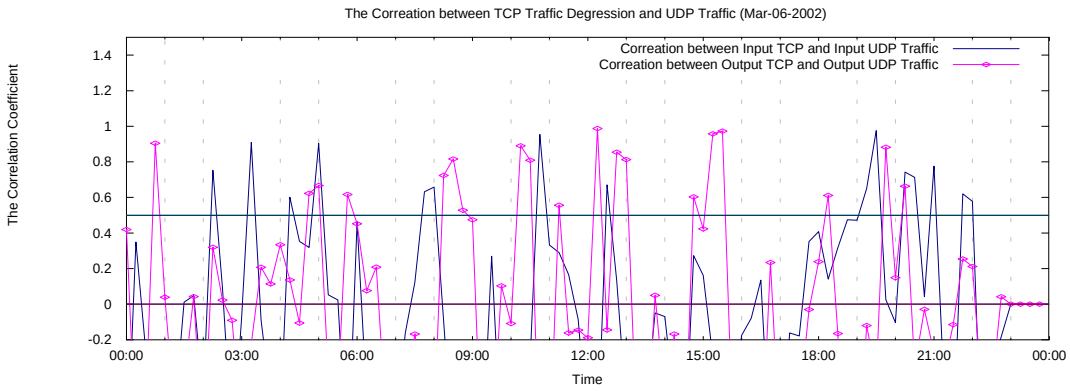
i = 0, 1, 2, ... , 144. n = 6.

where $(S_{xx})_i = \sum_{i}^{i+n}(x_i - \bar{x})^2$,

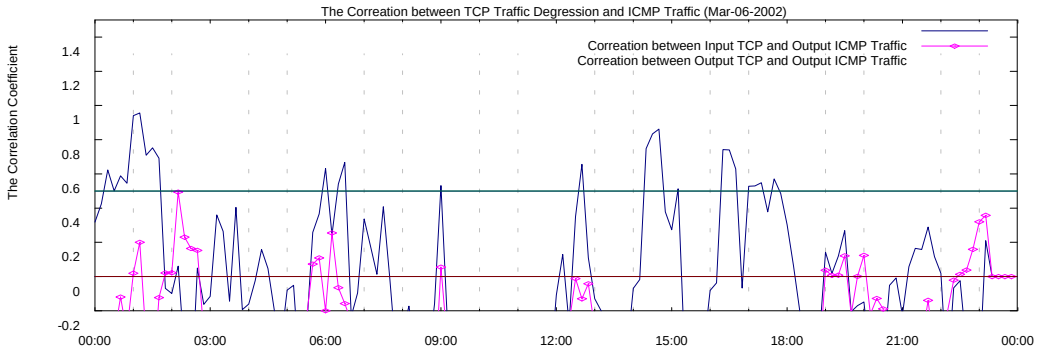
$$(S_{yy})_i = \sum_{i}^{i+n}(y_i - \bar{y})^2,$$

$$(S_{xy})_i = \sum_{i}^{i+n}(x_i - \bar{x})(y_i - \bar{y})$$

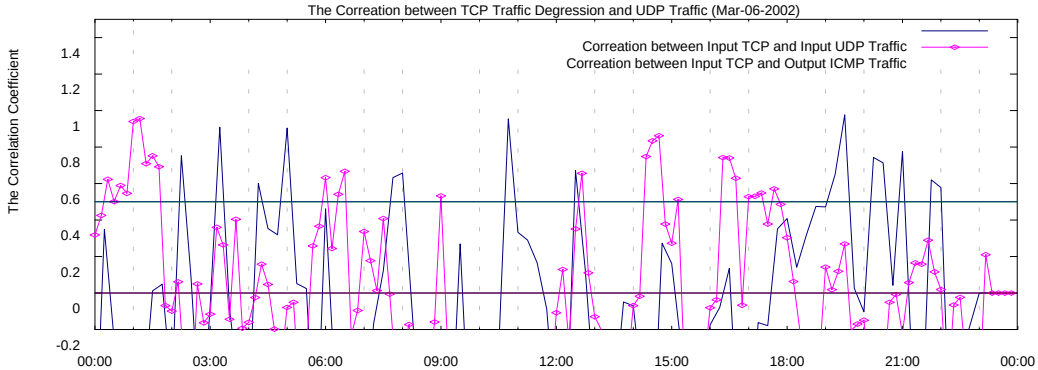
Fig.5a 顯示統計的國外 TCP Traffic Degression 與 UDP 訊務迴歸相關係數分布. 訊務尖峰時段的 UDP 訊務與 TCP Traffic Degression 明顯相關出現於 8:00-9:00, 10:30-11:00, 19:00-19:30, 20:30-21:00, 21:30-22:00 時段.而 Traffic Degression 與 ICMP 輸出訊務的明顯迴歸相關出現於: 1:00-1:40,14:00-15:00, 16:30-18:00 時段. 顯然, 持續 burst 訊務時段的 ICMP 訊務明顯相關於 TCP Traffic Degression Degression,而扁平分布的非自律 UDP 訊務也與訊務尖峰的 TCP Traffic Degression 明顯相關. 整體而言, ICMP/UDP 交互影響 TCP Traffic Degression (Fig. 5c).



(a)



(b)



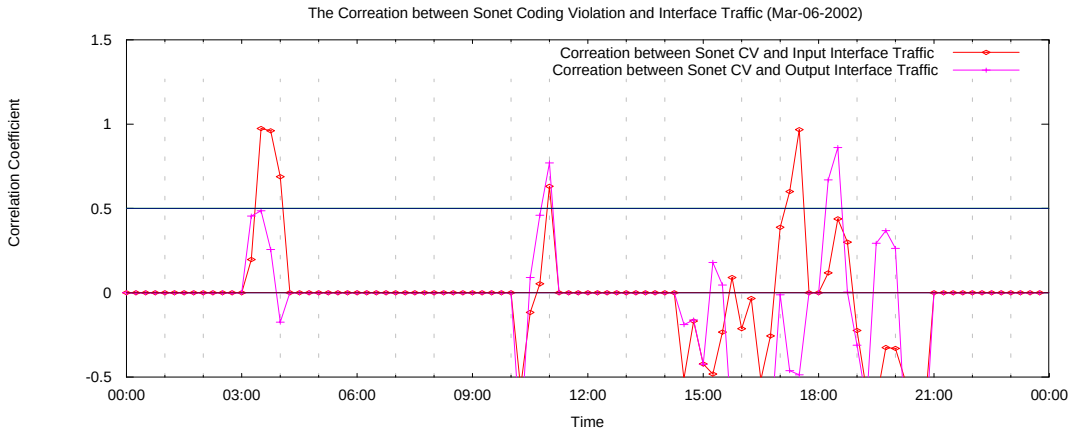
(c)

Fig. 5. 國外連線 TCP Traffic Degression 與 UDP/ICMP 訊務的相關

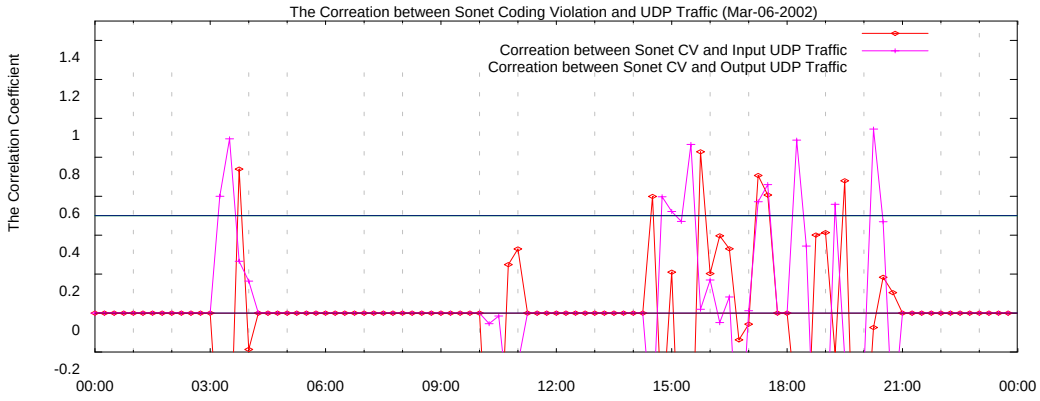
4.2. UDP/ICMP 訊務與 Sonet CV 的相關

為觀察國外 OC3 Link UDP/ICMP 訊務與 Sonet CV 傳輸錯誤變量的相關, 我們利用整體 Interface 訊務量,UDP 訊務量, ICMP 訊務量與 Sonet CV 頻次等數據, 取樣每 4 個時間單元 (per 15-min), 分別 計算 Sonet CV 與 Interface 訊務, UDP/ICMP 訊務的迴歸相關係數.

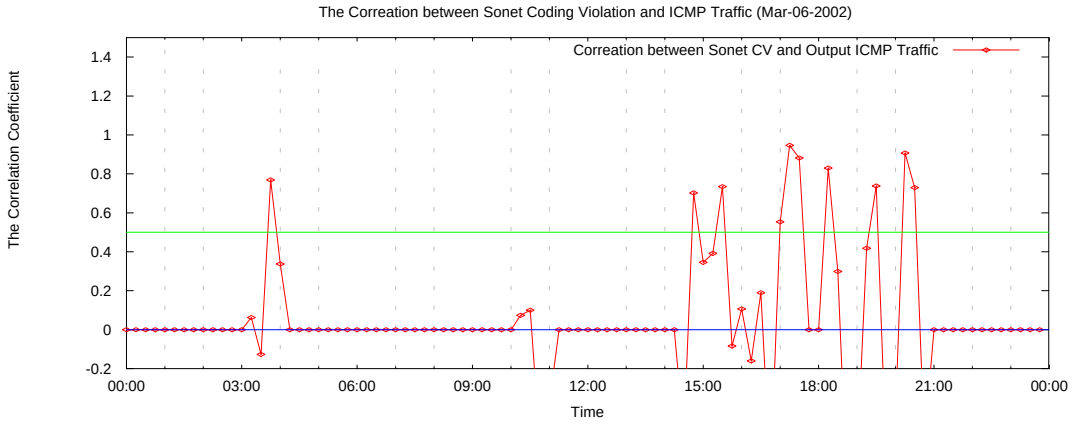
統計數據顯示: 整體 OC3 Interface 輸入訊務與 Sonet CV 間的明顯相關出現於 3:15 - 4:00, 11:00, 17:00- 17:30, 18:00 - 18:30 (Fig.6a). 而 UDP 訊務與 Sonet CV 間的明顯相關出現於 3:30, 14:30-15:30, 17:00-17:30, 20:30 (Fig.6b). Sonet CV 與 ICMP 訊務的迴歸相關數據則顯示: ICMP 輸出訊務與 Sonet CV 變數兩者間的明顯相關出現於 3:45, 14:30-15:30, 17:00-18:00, 19:00, 20:30 時段(Fig.6c). 整體而言, Sonet CV 高峰時段明顯相關於 UDP 與 ICMP 訊務.而 competitive UDP/ICMP 與 Sonet CV 頻次的相關高於 Interface 總介面訊務與 Sonet CV 頻次的相關.



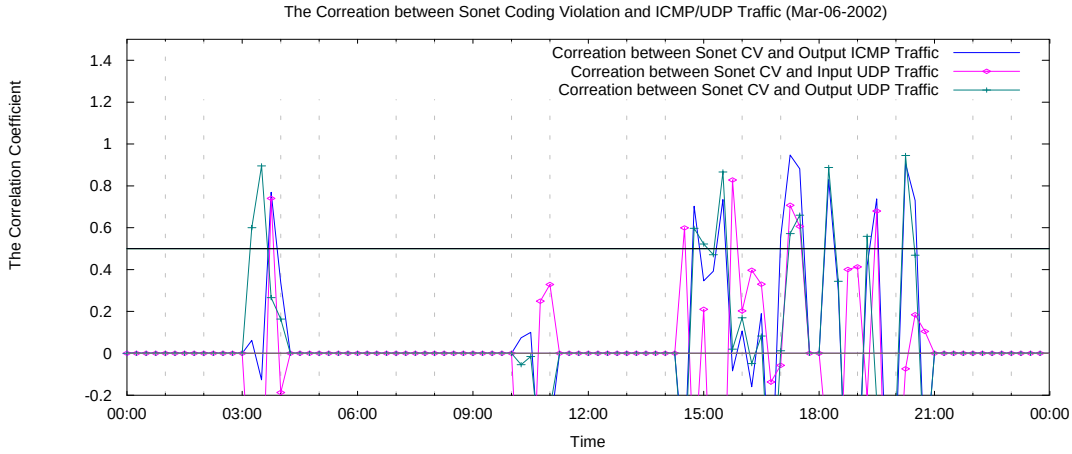
(a) SONET Coding Violation 與 Interface 訊務的相關



(b) SONET Coding Violation 與 UDP 訊務的相關



(c)SONET Coding Violation 與 ICMP 訊務的相關



(d) SONET Coding Violation 與 ICMP/UDP 訊務的相關

Fig. 6. TANet 國外連線 SONET Coding Violation 與 ICMP/UDP 訊務的相關

5. 結論

TANet 國外連線為國內學術研究機構連上國際網路的最主要途徑,隨著國外訊務的迅速成長, TANet 國外連網訊務也迅達飽和使用狀態. 本研究實做的 Sonet 傳訊品質與承載的 TCP/UDP/ICMP 訊務量測,旨在透過 SNMP MIB pooling 及 netflow 轉送訊務 log 的分析,除了能協助用戶監測實際的 TANet 國外連線狀況.我們也依據統計的 TCP/UDP/ICMP 訊務數據與 Sonet CV 傳輸錯誤分布數據,計算 UDP/ICMP 訊務與 Sonet CV,及 UDP/ICMP 訊務與 TCP Degression 訊務變量間的迴歸相關係數.

統計數據顯示: 除了訊務尖峰出現較頻繁的 TCP traffic degression 外, 整體的 TANet 國外連線傳訊尚維持正常. 而幾個持續的 ICMP burst 訊務則明顯與 TCP Traffic Degression 及 Sonet CV 相關.而 UDP/ICMP 訊務與 Sonet CV 的相關也明顯高於整體 Interface 訊務量與 Sonet CV 頻次的相關.

除了網路偵錯 ping 與 traceroute 訊務外, ICMP 訊務並不承載網路應用封包. 但惡意的網路攻擊程式會同時建立大量的 ICMP 連接,快速傳輸無用的封包,企圖癱瘓網路服務主機或連網訊務. 依據 ICMP burst 訊務與 Sonet CV 頻次/ TCP degression 的明顯正相關,可以了解 Internet 管理人員普遍在骨幹 router 設定有限

頻寬,分頻管制 ICMP 訊務的原因.Internet 用戶也可以了解: 藉由 ping, traceroute WAN 網路所回應的 Round Trip Time (RTT)訊息,已經無法反應實際的連網狀況.

參考文獻

(1) William Stallings, Networking Standards – A Guide to OSI, ISDN, LAN, and MAN Standards, Addison-Wesley, 1993.

(2) Request for Comments 2558, Definitions of Managed Objects for the SONET/SDH Interface Type, Network Working Group, March 1999.

(3) Bruce G. Barnett & Emilie T. Saulnier E. T.,High Level Traffic Analysis of a LAN Segment, Local Computer Networks, 1992. Proceedings., 17th Conference on , 1992, pp 188 –197.

(4) Takayuki Kushida, The traffic measurement and the empirical studies for the Internet, GLOBECOM, Volume 2, 1998, pp 1142-1147.

(5) Kevin Thompson, Gregory J. Miller, Rick Wilder, Wide-Area Internet Traffic Patterns and Characteristics, IEEE Network, Nov/Dec, 1997, pp 10-23.

(6) Cisco IOS Netflow Technology, http://www.cisco.com/warp/public/cc/pd/iosw/ prodlit/iosnf_ds.htm.

(7) flow-tools: Tool set for working with NetFlow data, http://freshmeat.net/releases/86475.

(8) Request for Comments 1157, A Simple Network Management Protocol (SNMP), Network Working Group, May 1990.

(9) Apache https server project, http://httpd.apache.org/ABOUT_APACHE.html.

(10) PHP: Hypertext Preprocessor http://www.php.net/manual/en/introduction.php.

(11) Walpole R. E. & Myers R. H., “Probability and Statisticis for Engineers and Scientists, MacMillan London, 1989.

(12) Strategies to protect Against Distributed Denial of Service (DDoS) Attacks, http://www.cisco.com/warp/public/707/newsflash.html..