1V－3 OC3monによるインターネットトラヒックの連続取得とそのリアルタイム処理に関する一検討

北辻 佳憲　堀田 孝男　藤長 昌彦　浅見 徹
株式会社KDD研究所

1. はじめに

155 Mbit/s (OC3) ATM回線上のインターネットトラヒックをキャプチャするシステムとして、MCI/ CAIDAによって開発/公開されているOC3monがある[1][2]。OC3monはIPヘッダをキャプチャしてファイルに書き込むものであり、これを事後解析することによりvBNS[3]等のインターネットバックボーンのトラヒック解析に利用されている。しかし、現在のOC3monはキャプチャしたデータを単一のファイルに出力するため、長期間の連続動作を行なうことができず、例えば、累積パケット数等の計測を行なうことができない。

本稿では、OC3monの機能拡張を行ない、連続動作を可能とするための出力ファイル切換え機能と、キャプチャデータをリアルタイムで処理することによる実時間トラヒック監視機能を追加した結果について述べる。

2. OC3monの概要

OC3monのハードウェアは、図1に示すように、OC3回線を分岐するスプリッタとATMセルを受信するための2枚のATMアダプタ、FreeBSDあるいはDOSが動作するPCからなる。ソフトウェア的には、アダプタ上で動作してATMセルのリアセンブリングを行なうファームウェア、アダプタを制御するデバイスドライバ及びユーザ空間で動作してデータをファイルに書き込むキャプチャプログラムから構成される。

アダプタで受信したATMセルは、ファームウェアによりAAL5フレームに組み立てられ、その先頭48バイトが、タイムスタンプ8バイト、フレーム先頭のATMセルのヘッダ4バイト(HEC除く)とともに、合計60バイトのレコードとしてデバイスドライバが管理するPCのメモリに書き込まれる。デバイスドライバでは、1Mバイトのブロックを単位としてメモリを管理しており、このメモリブロックが76バイトのブロックヘッダと17475レコードで満されるとキャプチャプログラムに通知する。キャプチャプログラムでは、デバイスドライバからの通知待ちとブロック単位でのファイルへの書き出しというループ処理を、シグナルによるユーザからの停止要求を受信するまで繰り返す。

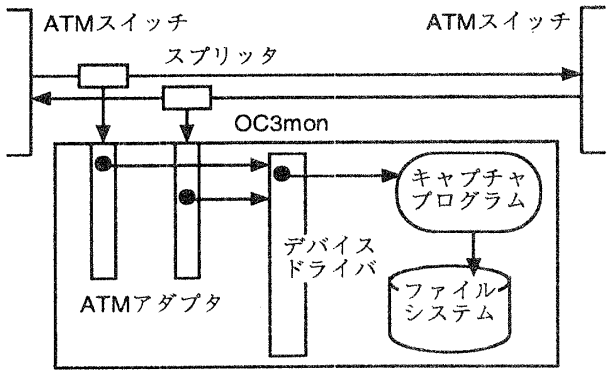

図 1: OC3monの構成

3. OC3monの機能拡張

OC3monを連続動作可能とするためには、定期的に出力ファイルを切換え、過去のファイルに対して必要なトラヒック解析を行なって、ファイルを消去あるいはCD-ROM等に保存すれば良い。一方、実運用の視点からは、ATM回線上のトラヒックを実時間で監視できることが望ましい。現在このようなツールとして、ルータからSNMPによりトラヒックデータを取得し、WEBページ上にグラフ化するMRTG (Multi Router Traffic Grapher[4])が広く利用されている。しかし、MRTGにおいてトラヒック測定の粒度を細かくするとルータへの負荷が重くなり、実ネットワークに影響を与える恐れがある。そこで、このような影響が生じないパッシブ型測定ツールであるOC3monの特徴を活かして、トラヒックデータの実時間処理を行ない、外部プログラムからの参照を可能とすることとした。

図2に拡張機能の構成を示す。OC3monのキャプチャプログラム(FreeBSD版)がキャプチャデータをファイルに出力した後、以下の処理を行なうよう改修した。

- 現在の出力ファイルの使用時間が予め指定された値を越えた場合、そのファイルをクローズして新しいファイルをオープンする。
- メモリブロック内のトラヒックレコードを走査し、ATMのVCごとにパケット数とバイト数を計測し

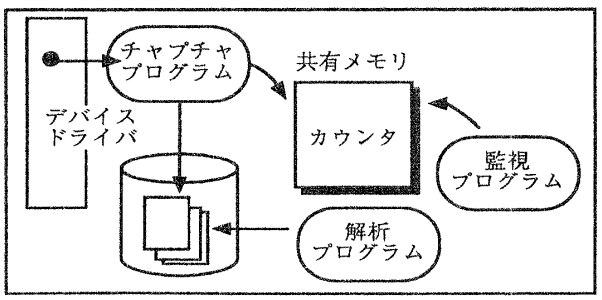

図 2: 拡張機能の構成

On continuous traffic capturing of the Internet and its realtime processing with OC3mon
Yoshinori Kitatsuji, Takao Hotta, Masahiko Fujinaga and Toru Asami
KDD R&D Laboratories Inc.

て、共有メモリ上に設けたカウンタをインクリメントする。

これにより、OC3mon の動作を中断することなく、別プログラムによるキャプチャファイルの解析/保存/消去と、ネットワーク機器へ負荷をかけないトラヒックの実時間監視が可能となる。

4. キャプチャ性能の評価

今回の機能拡張は、キャプチャプログラムに新たなルーチンを追加する形で実現した。このため、キャプチャプログラムとしての性能の劣化が懸念される。そこで、改修した OC3mon を用いて実トラヒックをキャプチャし、それに要する時間を測定した。

測定方法として、キャプチャプログラムのループ処理内で、デバイスドライバからの通知を受けた直後の時刻と、ブロックに対する処理を完了してデバイスドライバからの次の通知待ちに入る直前の時刻を gettimeofday() システムコールにより取得し、両者の差を処理時間とした。測定は 7200 秒間行ない、240 秒ごとにファイルを切換える設定とした。なお、OC3mon として使用した PC は、450 MHz の Pentium II プロセッサと 128 M バイトのメモリを有するものである。

測定の結果、処理時間の最小値、平均値及び最大値は、各々20、35、220 msec であった。図 3 に、処理時間の分布を示す。測定時間中 310 回のファイルへの出力と、28 回のファイルの切換えが発生した。図 3 において 140 msec 程度の処理時間を要しているものの多くが、ファイル切換えを行なった場合のものであった。

測定結果から、平均 35 msec で 17475 レコードを含むブロック、即ち約 500 K パケット/秒を処理可能であることが分る。文献 [1] によれば、現在のインターネットにおける平均パケット長は約 250 バイトであることから、双方向で 1 Gbit/s、片方向で 500 Mbit/s まで処理可能であり、155 Mbit/s の ATM 回線に充分対応できる。

5. 考察

(1) 現在のインターネットにおいては、HTTP や FTP 等、TCP 通信が支配的である。この時、IP パケットは、最小でも IP ヘッダ 20 バイト、TCP ヘッダ 20 バイトの 40 バイトからなり、これに LLC/SNAP の 8 バイトヘッダと AAL5 の 8 バイトトレーラが付加されるため、少なくとも二つの ATM セルに分割されると考えてよい。従って OC3 回線における IP トラヒックの上限は、片方向 183K パケット/秒、双方向でも 366 K パケット/秒となる。今回の測定では、平均で 500 K パケット/秒を処理可能であることから、OC3 回線に充分対応可能と考えられる。

(2) ファイルの切換え (旧ファイルのクローズと新ファイルのオープン) 処理が発生した場合、140 msec から最大 220 msec の処理時間を要する。FreeBSD におけるファイル I/O 及びプロセススケジューリング、その時点での他のプロセスやバッファキャッシュの状態等により変動するが、トラヒックが 366 K パケット/秒でファイルの切換えに 220 msec 要したとすると約 80,000 パケット分の未処理レコード (約 5 M バイト) がメモリに蓄積される。この後 366 K パケット/秒のトラヒックと未処理分を 500 K パケット/秒で処理するとすると、約 0.6 秒で未処理分を解消することができる。即ち、ファイルの切換え間隔を 1 秒以上に設定すればよいと推測できる。

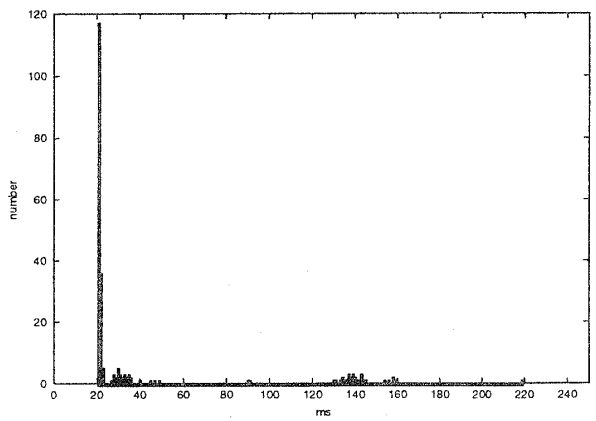

図 3: 処理時間の分布

6. おわりに

155 Mbit/s(OC3) の ATM 回線上のインターネットトラヒックをキャプチャする OC3mon に、出力ファイルの切換え機能を追加して連続動作を可能とするとともに、トラヒックデータをリアルタイム処理して VC ごとのパケット数、バイト数を計測する機能を実現し、外部からの参照を可能とした。また、これらの機能を付加した OC3mon を実ネットワークに接続し、OC3 回線に充分対応可能であることを確認した。

今後は、長期的な実インターネットトラヒックのキャプチャを行うとともに、VC のトラヒックを観測して予め指定された変化が現われたときに管理者へ通知する等の機能を提供する監視プログラム、種々のトラヒック解析プログラムの作成、OC12mon への本拡張機能の適用等を検討する予定である。

最後に、日頃ご指導戴く KDD 研究所村谷所長、鈴木、山本両副所長に感謝する。

参考文献

[1] National Laboratory for Applied Network Research, http://www.nlanr.net/NA/Oc3mon/
[2] Cooperative Association for Internet Data Analysis, http://www.caida.org/Tools/CoralReef/
[3] very high performance Backbone Network Service, http://www.vbns.net/
[4] Multi Router Traffic Grapher, http://ee-staff.ethz.ch/ oetiker/webtools/mrtg/mrtg.html