5E−6

TCPセッションを考慮したパケットモニタリングツール

山根 健一　　矢吹 道郎
上智大学

1 はじめに

インターネットの需要が高まっている現状において,インターネット上でのデータの流れを理解することはもちろん,統計を取り解析を行なう必要がある.現在,モニタリングツールは複数存在しているが,TCPのセッション単位でのモニタリングツールは一般的に知られていない.TCP/IPはインターネットアーキテクチャの重要な機構であり,数多くのネットワークソフトウェアにこの機構が利用されている.TCPのセッション単位でのモニタリングをすることにより,TCPの理解を深めることはもちろん,TCPの再送などを中心としたトラフィックの解析にも役立つであろう.本論文では上記の機構を採り入れたモニタリングツールを紹介する.

2 セッション単位でのモニタリング

TCPはインターネットアーキテクチャの重要なプロトコルである.様々な通信ソフトウェアに用いられており,インターネットの研究者はその機構を理解し,有効的な利用を心がけなければならない.しかしながらTCPは複雑であり,コネクション指向ゆえにコネクションの確立,終了または信頼性の確保のためなど様々の状態が遷移する.また効率の良い通信を行なうためのウィンドウ制御もなされている.

セッション単位でのモニタリングツールを考えた時に,トラフィックの統計,解析の面から考えると,セッション単位での解析ができ,さらに再送に注目することができることにより今までにない統計,解析が行なえるであろう.

また教育的な面から考えると,セッションでのパケットの流れが分かるのでTCPの様々な状態遷移をつかむことができる.またTCPの再送がどのような時に起こるのか,ウィンドウ値の変化などが容易に理解できる.

本研究ではこのような必要性からTCPのセッション単位でのモニタリングツールを開発した.

3 機能と構成

セッション単位でのモニタリングを行なうには,まず,パケットデータの中にどのようなセッションがあるか,また,それらがどのようなセッションであるかをユーザに示さなければならない.これによりユーザは解析をするセッションを選択することができる.セッション単位の情報としては,通信ホスト,データグラム数,再送数などの統計データが示される.次に選択されたセッションの表示を行なう.セッションの表示では通常のパケットデータの表示に加えて,通信方向,あるいは再送などが重要になってくるため,本ツールもそれに対応した表示方法をとっている.

本ツールではセッション単位でのモニタリングと取り出したパケット順に表示する通常のモニタリングの機能を提供している.どちらの構成もデータを取り込む部分と出力する部分とに分かれている.データを取り込む部分はSunのネットワーク・インタフェース・タップを使用している.出力形式の指定においては,ユーザは記述ファイルを介して,必要な情報だけを選択するなど自由な設定が可能となっている.

現在,データを取り込む部分と出力する部分と

Packet Monitoring Tool with capability of TCP session handling
Ken'ichi YAMANE, Mitchirou YABUKI
Faculty of Science and Technology, Sophia Universty

を分けている.理由は,セッションの選択を行なうため,および処理の負荷が大きいためである.

4 モニタリングツールの利用

セッション単位でのモニタリングは最初に各セッションの統計データを表示する.この表示は図1に示す.表示ではセッション中の全パケット数,再送が起こった回数などが表示される.また,セッションが完全に終了,未終了の表示もされている.次にセッション番号を指定してセッションの内容を表示する.図1のセッション番号13を選択した場合の例を図2に示す.ここでは各ヘッダの内容また各パケットの通信方向,再送（図の[R]で示されている）なども含めて表示される.

5 まとめ

本研究では,TCPのセッション単位でのモニタリングツールを作成した.これによりユーザがTCPを理解する助けになるであろう.また再送に注目したトラフィックの統計にも役立つであろう.

データを取り出す部分と出力する部分を分割しなければならないところから,リアルタイム性に欠けるという欠点がある.今後,リアルタイムのモニタリングへ開発を進める予定である.

参考文献

[1] Postel, J.B. *Internet Protocol.* RFC 791, September 1981.

[2] Postel, J.B. *Internet Control Message Protocol.* RFC 792, September 1981.

[3] Postel, J.B. *Transmission Control Protocol.* RFC 793, September 1981.


```
                    START TIME 93/8/1 23:00:11
------------------------------------------------------------------------
                                SESSION NUMBER = 8    [not finished]
SESSION START TIME 93/8/1 23:15:58.107.489
        ETHER     src 08:00:20:07:dd:2c      dst 08:00:20:0e:1b:41
        IP        src uranus     dst eseg
        TCP       src 1159       dst untp
TOTAL PACKETS = 1178
TOTAL RETRANS = 21
                                RETRANS STAT :     21[1]
FROM      uranus   TO              eseg :     21[1]
FROM      eseg     TO            uranus :      0[1]
------------------------------------------------------------------------
                                SESSION NUMBER = 13    [finished]
 SESSION START TIME 93/8/1 23:17:02.477.225
          ETHER     src 08:00:20:00:8e:ff      dst 08:00:20:08:b1:c3
          IP        src kiyoshi    dst 133.12.11.21
          TCP       src ftp-data   dst 3864
 TOTAL PACKETS = 11
 TOTAL PACKETS = 1
                                RETRANS STAT :      1[1]
 FROM       kiyoshi  TO       133.12.11.21 :      0[1]
 FROM   133.12.11.21 TO            kiyoshi :      1[1]
 SESSION LAST TIME   93/8/1 23:17:02.545.881
------------------------------------------------------------------------
                                  ⋮
```

図 1: セッション選択時の表示

```
                    START TIME 93/8/1 23:00:11
                    SESSION NUMBER = 13
  Time 93/8/1 23:17:02.477.225              ether_length      60
       ETHER src 08:00:20:00:8e:ff      dst 08:00:20:08:b1:c3
 --->  IP    src kiyoshi  dst 133.12.11.21          ip_length      40
       IP    id  15576    off 0    ttl 30
       TCP   src ftp-data dst 3864 seq  1200321     ack            0
       TCP   off 5        win 4096     flags SYN
  Time 93/8/1 23:17:02.480.041              ether_length      60
       ETHER src 08:00:20:08:b1:c3      dst 08:00:20:00:8e:ff
 <---  IP    src 133.12.11.21     dst kiyoshi      ip_length      44
       IP    id  10073    off 0    ttl 59
       TCP   src 3864 dst ftp-data seq  1752256000  ack      1200322
       TCP   off 6        win 24576    flags SYNIACK
       TCP   option       Maximum Segment Size     1460[bytes]
                                  ⋮
  Time 93/8/1 23:17:02:523.037              ether_length      60
       ETHER src 08:00:20:08:b1:c3      dst 08:00:20:00:8e:ff
 <---  IP    src 133.12.11.21     dst kiyoshi      ip_length      40
       IP    id  10075    off 0    ttl 59
       TCP   src 3864 dst ftp-data seq  1752256001  ack      1201462
       TCP   off 5        win 23437    flags ACK
[R] Time 93/8/1 23:17:02:531.713          ether_length      60
       ETHER src 08:00:20:08:b1:c3      dst 08:00:20:00:8e:ff
 <---  IP    src 133.12.11.21     dst kiyoshi      ip_length      40
       IP    id  10076    off 0    ttl 59
       TCP   src 3864 dst ftp-data seq  1752256001  ack      1201462
       TCP   off 5        win 24576    flags ACK
                                  ⋮
```

図 2: セッションの表示