2004－DSM－34　(6)
2004／7／30

通信トラフィック監視システムの試作と バーストトラフィックの検出

水越一貴[1]　牧野晋[2]　林英輔[2]

ネットワークのトラフィック監視には The Multi Router Traffic Grapher (MRTG)が広く使われている．MRTG では 5 分，30 分，2 時間，1 日平均のトラフィックが検出可能である．しかしこのシステムでは短時間の大量トラフィック，通称バーストトラフィックの検出は固定された平均時間による平滑化によって，通信トラフィックを実状に近いデータとして観測することは困難である．そこで任意時間平均のトラフィック量を検出することが可能なトラフィック監視システムを試作した．このシステムを使って千葉県館山地区で行われた総務省の無線 LAN の実証実験においてバーストトラフィックの検出を行って平滑化されないデータ監視を実現した．

The trial production a communication traffic surveillance system and burst traffic detection

MIZUKOSHI Kazutaka,†1 MAKINO Susumu,†2 and HAYASHI Eisuke†2

The Multi Router Traffic Grapher (MRTG) is widely used for the traffic surveillance of a network. In MRTG, average over several time intervals, such as 5 minutes, 30 minutes, 2 hours, and one day. However, it is difficult for detection of short-time extensive traffic and common-name burst traffic to observe communication traffic as data near the actual condition by flat and smoothen by the fixed average time in this system. Then, the traffic surveillance system, which can detect the amount of traffic of an arbitrary time average, was made as an experiment. The data surveillance, which detects burst traffic in the actual proof experiment of the wireless LAN of the Ministry of Public Management, Home Affairs, Posts and Telecommunications conducted in the Chiba Tateyama division using this system, and it is found out that we get real traffic data, which are not flat and not smooth.

†1 麗澤大学大学院国際経済研究科
Graduate School of Economics and Business administration, Reitaku University
†2 麗澤大学国際経済学部
The International School of Economics and Business administration, Reitaku University

１．はじめに

通信トラフィックの監視は，ネットワーク運用管理上で最も重要なタスクである．ネットワークシステムの性能の調査やセキュリティ管理では，通信トラフィックが監視対象になることが多い．ネットワークシステムの利用状況は，それが適正な利用であっても，不正な利用であっても，通信トラフィックに反映される．そのためシステムの運用上，同システムの各所の通信トラフィックを測定し，このデータを収集・分析しておくことは，ネットワーク障害やウイルス攻撃などを検知する手がかりになる．このようなことから通信トラフィックを監視することはシステム運用組織に常に課される任務であるといえる．

現在，ネットワークのトラフィック監視では，The Multi Router Traffic Grapher (MRTG)[1]が使われることが多い．MRTG は標準で 5 分ごとに監視対象へポーリングしてトラフィックデータを収集して，1 日（5 分平均），1 週間（30 分平均），1 ヶ月（2 時間平均），1 年（１日平均）における時間帯平均値の推移のグラフを作成表示する．これらのグラフは，上述のような時間範囲にわたる平均値であるため，いわゆる曲線の平滑化効果が行われるためより短時間にトラフィックの変化をそこから観察することは不可能である．例えば，5 分間のうちの 1 分間に１MB/bps のトラフィックがあったとしてもその他の 4 分間にトラフィックがない場合，２００KB/bps のトラフィックとなってしまう．

近年のネットワークでは高帯域化が進み，短時間に数十 MB のトラフィックが流れることが起こりうる．ポーリング間隔において数十 MB 単位のトラフィックが発生した場合，MIB[2]のカウンタ溢れが起ってしまい，5 分間隔では正常なトラフィック量を測定することはできない．そのような場合，タイムインターバルをより短い，適切な時間に設定することができればカウンタ溢れが起こったことも検知できより正確なトラフィックを測定することができる．

また，MRTG では後日，解析や検証を行おうことが難しい．なぜならば，必要なトラフィックが発生したその日のうちにデータを取得しておかなくては平滑化が進んでしまうために 5 分単位での 1 日のデータを使うことができないからである．

そこで本研究では，ポーリングのタイムインターバルを任意に設定することができるトラフィック監視システムを試作した．また，同システム上にこのシステムを用いることにより運用環境や実験環境においてより適切なトラフィックを測定することが可能になる．また，取得したすべてのデータを残すことによって，後日になってからも検証を行うことができる．

以下，2 章では，トラフィック監視システムに求められる課題や構成について述べる．3 章では，試作したシステムを用い，千葉県館山地区で行われた総務省の無線 LAN 実証実験のトラフィックを測定したことについて述べる．4 章では，実験のトラフィック測定から得られた結果を考察し，5 章でまとめを行う．

２．トラフィック監視システムの試作

本研究では，トラフィック監視システムに求められるシステム要求や構成について検討し，システムを試作した．また，試作したシステムを用い測定実験を行った．

2.1 システム要求

MRTG は SNMP[3]を用いて監視対象を一定時間ごとにポーリングすることによってトラフィックを測定している．一定時間は通常 5 分となるためにデータも 5 分平均となる．表示されるグラフも 1 日が 5 分平均のデータで描かれることになる．

同システムでは，MIB にアクセスして獲得されて保存されるデータは，ラウンドロビン管理により保存領域の肥大化を防ぐため，1 日以上経過したデータは合併され，より大きな単位時間にわたる平均値に変換されて保存される．

これらのことから次の問題が発生する．

- 5 分ごとにポーリングしているため 5 分平均のデータになる
- 分析するツールがグラフしか作れない
- データベースがラウンドロビン管理されているために古いデータから平滑化され消されてしまう

このような問題を解決するために，本研究のシステムには，次のような機能を持たせることにした．

- 任意時間間隔で MIB にアクセスしてデータを取り出す
- データの取り出しと分析をするプログラムを別々にして，お互いに独立なサブシステムとして開発する
- MIB から取り出したデータはすべて内臓ディスク上に保存し，随時に部分集合を参照できるようにするため，データベースを構成する

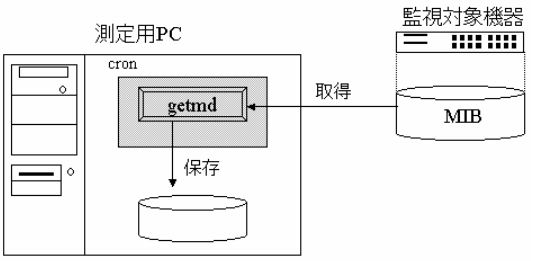

図１　システムの構成
Fig.1 System configuration

上記の機能を具備することにより，随時に本システムをポーリングすることによって任意に指定した時間帯のデータ集合を取得し，図形処理によりグラフを作成したり，データ集合のみを別分析に利用したりすることができるようになる．

2.2 システム構成

ネットワークトラフィックは，ルータやスイッチ等の監視対象機器の MIB を参照して測定する．MIB には，通過したパケットの累和が格納されているので，SNMP を用いて取得する．取得された時系列データの隣り合う要素の差分から，その機器のデータ通信速度，すなわちデータ伝送速度を得ることができる．

システムの構成を図１に示す．SNMP により MIB からデータを取得するプログラム getmd を作成し，測定用の PC にプログラムを組み込んだ．Linux 上の cron を用いて getmd を実行し任意時間に MIB データの取得が行えるようにする．得られたデータをそのままファイルへ保存し，ファイル名は保存された日付として，内容は取得時間と値になる．

開発直後は cron の設定を１分とした．この設定では，保存されるファイルの容量は 1 分

間隔で MIB から取得するので input と output を合わせて 1 ヶ所 1 日１００KB 程度となる．よって，４０MB 程度で 1 年間のデータを保存することができる．なお，cron 設定は，必要に応じて分単位で変更することができる．

2.3 試作システムの検証実験

試作したシステムを用い測定実験を行った．実験の構成を図２に示す．

HUB のある指定したポートに流れるトラフィックを測定する．トラフィックの測定は，MRTG でも行い比較する．実験として PC A から PC B に５MB のデータを 3 分ごとに計 5 回 FTP した．MRTG のポーリングは一般的な５分とし，試作システムは１分として測定した．

その結果から MRTG で測定した図 3 と試作したシステムで測定した図４を示す．MRTG では５回試行した結果が１回のように見えるが試作したシステムでは，５回試行されている様子がわかる．また，MRTG では最大値が３００kbits/sec 程度であるのに対し試作システムでは，７１０kbits/sec 程度であり，２倍以上の差が生じている．

これらのことから試作したシステムはより正確なトラフィックを計測できることがわかる．

３．実用実験としての館山実験[4]

前章で試作したトラフィック監視システムを千葉県館山地区にて行われた総務省の無線 LAN の実証実験においてトラフィック測定用として利用した．

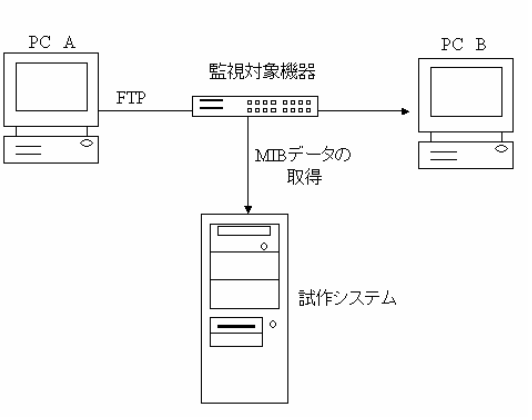

図２　試作システムの測定実験構成
Fig.2 Trial production system measurement experiment composition

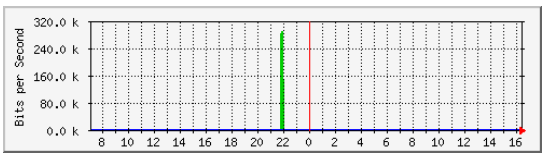

図 3　MRTG トラフィックデータ
Fig.3 MRTG traffic data

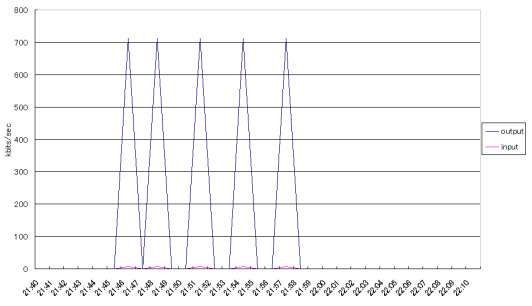

図 4　試作システムトラフィックデータ
Fig.4 Trial production system traffic data

3.1 実験の構成

総務省の無線 LAN の実証実験として行われた千葉県館山市内の実証実験対象の２地区で行われた実験運用において 2004 年 3 月 17 日 13 時からトラフィックの測定を開始し，測定はその後も継続している．

館山地区においてネットワークが平砂浦地区と神余地区の 2 つに分かれているのでそれ

ぞれの上位にある L3 スイッチのポートを監視した．(図５)

トラフィック監視システムサーバ（取得用マシン）として使用機器（ハードウェア）用自作 PC の仕様主要部は以下のようである．

CPU : Pentium4 2.4GHz
RAM : 1GB
HDD : 80GB

トラフィック負荷実験の入力地点であるホテルアクシオンのロビーでは，末端の IEEE802.11g 無線 LAN に数台のノート PC を用いて一斉に，館山のネットワークからインターネット越しに麗澤大学の実験用に設置された Web サーバから１MB，５MB，１０MB，３０MB のファイルを任意にダウンロードした．この負荷実験は３月１７日１３:００から１５:００へかけて実施された．トラフィック監視システムは，その後もデータ収集を継続し，収集したデータは，同ネットワークを運用している南房総 IT 推進協議会（NPO）にグラフの形で提供されている．

3.2 実験結果

実験時間全体において１つの地区あたり約 24KB のテキストデータベースが得られた．

得られたトラフィックデータから平砂浦地区の実験時間中全体の input トラフィックデータ図６と output トラフィックデータ図７を作成した．ここでは，個々のファイル転送における幅数十秒のスパイク状になっているトラフィック曲線数個の重なりの様子が実状に近い形で再現されていることが分かる．

この負荷実験において，Web サーバのアクセスログからダウンロードされたファイルの容量と個数を表１に示す．

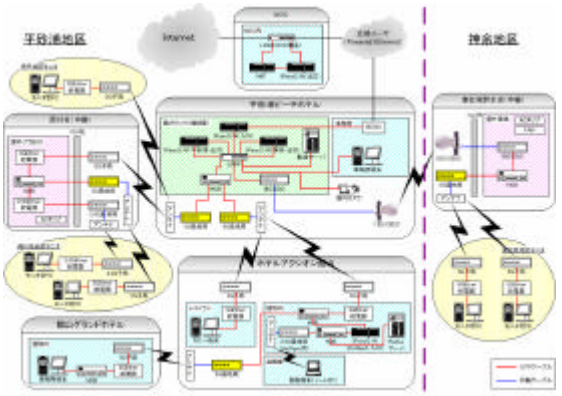

図５　館山無線ネットワーク構成概念図[4]
Fig.5 Tateyama Wireless network construct

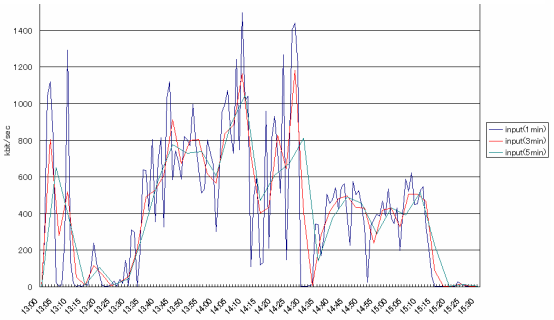

図６　平砂浦地区 input トラフィックデータ
Fig.1 input traffic data of Heisaura area

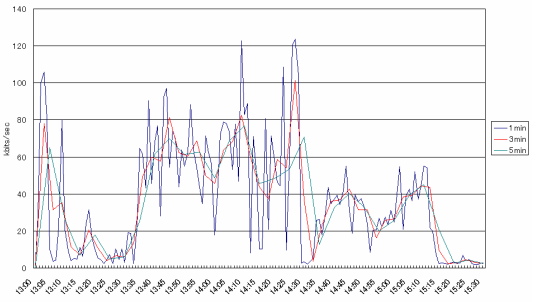

図７　平砂浦地区 output トラフィックデータ
Fig.7 output traffic data of Heisaura area

４．考察

図６より 13 時 10 分，45 分，14 時 10 分，25 分付近において 1 分平均と 5 分平均では倍

表１　ダウンロードされたファイル容量と個数
Table.7 downloaded the file capacity and the number

	ダウンロードされたファイルの容量				
時間	1MB	5MB	10MB	30MB	50MB
13:00-13:09					1
13:10-13:19					
13:20-13:29	1				
13:30-13:39	5	4			
13:40-13:49	11	1	2		
13:50-13:59	5	4	3		
14:00-14:09		8	3		
14:10-14:19	4	4	3		
14:20-14:29	3		2	1	
14:30-14:39	7			1	
14:40-14:49	9				
14:50-14:59	1	3		1	
15:00-15:09	10			1	
15:10-15:19				1	

程度の差が生じていることが分かる．

ポーリング間隔を短くするほど実状に沿ったトラフィックパターンになることが分かる．

また，表１も合わせて見るとトラフィックが高くなっている時間に多くのアクセスが発生していることが分かる．

５．おわりに

本論では，まず，現状のトラフィック監視システムの問題点を示した．次にこの問題を解決する手法として，タイムインターバルを任意に設定できるトラフィック監視システムを試作した．このシステムによって実際に発生しているトラフィックに近いデータを取得できることを検証した．また，実際に千葉県館山市内で行われた無線 LAN の実証実験において監視を行った．その結果，MRTG には現れないバーストトラフィックを測定することができた．

しかし，現在は cron を用いてタイムインターバルを設定しているために分単位でしか測定することができない．今後，システム自身で MIB アクセスの時間間隔を制御して，より短い間隔でアクセスできるようにすることが課題である．

また，結果の表示方法や複数箇所の同時ポーリング，ポーリングパケット自身のトラフィック量に対する影響等について検討してく予定である．

参考文献

[1] MRTG http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

[2] K. McCloghrie and M. Rose: “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”, RFC1213 (1991).

[3] J. Case, M. Fedor, M. Schoffstall and J. Davin: “A Simple Network Management Protocol (SNMP)”, RFC 1157 (1990).

[4] 総務省関東総合通信局：「ラストワンマイル克服のための最適アクセスシステムのあり方とセキュリティに関する調査研究会」報告書　(2003年7月)

[5] 山本成一,江崎浩．フローを意識したトラフィック解析のための基礎実験，情報処理学会報告 2004-DSM-33，pp.35-39，(2004-5).