2005－QAI－14（5）
2005／1／19

RTT分布と頻度に基づいたネットワークトラヒック解析

阿部　勝久†　　キニグレン マンスフィールド††　　白鳥　則郎†††

† 東北大学大学院情報科学研究科，株式会社サイバー・ソリューションズ
980–8577 仙台市青葉区片平 2–1–1，989-3204 仙台市青葉区南吉成 6–6–3
†† 株式会社サイバー・ソリューションズ
989-3204 仙台市青葉区南吉成 6–6–3
††† 東北大学電気通信研究所
980–8577 仙台市青葉区片平 2–1–1
E-mail: †abekatsu@cysol.co.jp, ††glenn@cysols.com, †††norio@shiratori.riec.tohoku.ac.jp

あらまし　ネットワーク計測は，ネットワークの性能を評価する際や運用の安定性・効率性を確保する上で必要不可欠な要素である。我々は，JGN–II ネットワークにおいてトラフィック情報を計測しつづけ，収集した値を研究対象としている。RTT は我々のネットワークトラフィック収集活動から得られる副次的統計情報である。RTT の計測値から，潜在的なネットワークの QoS やネットワーク容量を推定する手がかりが得られる。本研究では，JGN–II ネットワーク上で計測した RTT 値の性質について説明を試みる。その際に，RTT 値を解析する際に用いられる方法について調査を行った。また収集した RTT 値の解析を行い，その解析がネットワーク状態の監視における有用性について評価を行った。

キーワード　ネットワーク管理，ネットワーク計測，RTT 計測

Network Traffic Analysis on the basis of RTT measurements.

Katsuhisa ABE†, Glenn MANSFIELD KEENI††, and Norio SHIRATORI†††

† Graduate School of Information Science, Tohoku University and Cyber Solutions Inc.
2–1–1 Katahira, Aoba–ku, Sendai 980–8577, 6-6-3 Minami-Yoshinari, Aoba–ku, Sendai 989-3204
†† Cyber Solutions Inc.
6-6-3 Minami-Yoshinari, Aoba–ku, Sendai 989-3204
††† Research Institute of Electrical Comunication, Tohoku University.
2–1–1 Katahira, Aoba–ku, Sendai 980–8577
E-mail: †abekatsu@cysol.co.jp, ††glenn@cysols.com, †††norio@shiratori.riec.tohoku.ac.jp

Abstract　Network monitoring is necessary to evaluate the performance and to ensure operational stability and efficiency. We have been monitoring traffic statistics for the JGN–II network and are studying the results. RTT is one of statistics we have collected as a byproduct of the monitoring activity. RTT values do carry some hints about the underlying network's quality of service and capacity. In this paper, we clarify the nature of the RTT statistics that we have collected for the JGN–II network and survey the techniques used to analyse RTT statistics. We then analyse the RTT–statistics and examine its utility in monitoring network status.

Key words　network management, network monitoring, RTT measurement

1. Introduction

Network Traffic Monitoring is an important aspect of network management and security. For example, we might observe the effects on the network traffic when an event, such as a network failure, an operational failure or a security incident has occurred. And we would know the predictive information about quality of service, throughput and so on.

We have been researching and developing techniques of analysis and providing traffic statistics at a "JGN–II monitoring project". In this project, we aim at providing network information for network administrator to management and

for network user to know network status in experiment.

To execute this monitoring project, we put 10 probes in JGN–II network and have been monitoring traffic statistics for that network (Table 1 in Sec. 3). And two different agents have been collecting traffic statistics from probes via SNMP.

In this paper, we focus on Round Trip Time (RTT). This measurement shows us the important information to evaluate network quality of service, conditions and other status. And there are many works about RTT, e.g. distance metrics, RTT distribution, etc. We use SNMP to collect traffic statistics. As a byproduct we also record the time taken for each SNMP query to complete. This gives us the "SNMP–RTT". In this work, we examine the usefulness of this statistice and we show the correlation between the SNMP–RTT and RTT measured by other tools.

This paper consists of the following sections. Firstly we define the Round Trip Time and consider the relationship of our monitoring measurement in Sec. 2. We describe our monitoring environment in Sec. 3. We show some techniques to analyze RTT in Sec. 4. We also consider the result of analysis here. Finally we present our concluding remarks and future plans in Sec. 5.

2. Definition for RTT

There are many tools such as *ping*, *traceroute*, *skitter*, *pchar* and other tools, to measure Round Trip Time (RTT in short). Here we consider what kind of statistics these tools measure. Firstly we clarify the definition of RTT.

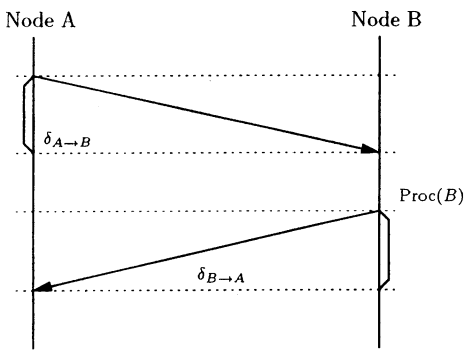

Fig. 1 diagram to measure Round Trip Time

Fig. 1 shows that the diagram of a packet flow. We simplify the Round Trip Time from node A to node B on single path as follows:

$$\mathrm{RTT}(A,B) = \delta_{A\to B} + \delta_{B\to A} + \mathrm{Proc}(B).$$

The first term ($\delta_{A\to B}$) stands for the time taken by the packet to transit from Node A to Node B, and the second term ($\delta_{B\to A}$) vice versa. The last term (Proc(B)) is the time that Node B takes to process the received packet and send the response packet.

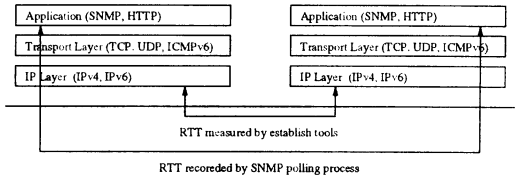

Fig. 2 the type of RTT depending on the measurement tools

The value of $\delta_{A\to B}$, we call it *transit time*, is reflected on the distance between two nodes. This value is influenced by the network status, such as capacity, available bandwidth and so on. Huffaker et al. deals with this issue [3].

On the other hand, *processing time*, Proc(B), depends on the time of packet such as ping, traceroute, SNMP polling and HTTP application. If the application to measure the RTT is changed, the change is reflected on processing time. For example, there must be difference between the processing time of HTTP application, time of SNMP access, and the time of ping. And it is easy guess that the simpler the measurement tool is, the shorter the processing time is. But with many measurement tools, it is difficult to measure these values separately. So we would like to know how to evaluate the processing time from these measurement tools.

As another matter, we also classify the type of RTT measured by the tools (Fig. 2). The estabilished tools, e. g., ping, traceroute and so on measure the IP-layer RTT. In this work, we use SNMP to collect traffic statistics. We also record the time taken for each SNMP query to complete, as a byproduct. We think that if the type of measuring RTT is changed, the different network information is provided.

3. Environment

In this section we describe our monitoring environment in JGN–II [1].

JGN–II is an open test-bed network environment for research and development and provides nationwide IPv6 network and optical wavelength networks in Japan.

We project a network traffic monitoring in JGN–II network. We aim at providing user network traffic information and analysis techniques to use for research and experiment in JGN–II network.

We adopt passive monitoring with splitter or tapping equipment for 100base–TX or 1000base–SX link. We have been placing probes at Miyagi, Tokyo, Gifu, Kyoto, Hirosihma and Saga, and polling traffic statistics from agents

on Sendai and Kyoto.

Table 1 shows our monitoring environment as on 26 July 2004. We place probes monitoring lines passively at all points in JGN-II. We use SNMP framework to collect traffic statistics. Two Polling Agents at Sendai and Kyoto periodically, every 60 seconds, access probes by SNMP over IPv6 and obtains traffic statistics which is obtained in the form of Managed Objects. We open these traffic information to the public [2].

Table 1 Monitoring Environment in JGN-II

Items	Number
Sites where probe is placed	9
Placed probes	10
Monitoring points	11
Monitoring links	26
(with VLAN)	(19)
Polling Agents	2

We show our monitoring traffic statistics on table 2. Here "other protocols" means that it is an IPv6 packet but its next header field is not ICMPv6, TCP or UDP. We also have been collecting Round Trip Time measured by traceroute6.

Table 2 Measuring statistics

IPv6 packets/traffic volume
ICMPv6 packets/traffic volume
TCP over IPv6 packets/traffic volume
UDP over IPv6 packets/traffic volume
Other protocols packets/traffic volume
SNMP Polling Interval
Elapsed time by Traceroute6

We provide cilckable map to show the traffic graph. The following example shows the traffic volume between Research Institute of Electric Communication in Tohoku University and the University of Tokyo on Fig. 3. In this way, user can know the network traffic statistics graphically.

4. Measurement Experiment

In this section, we introduce our experiment and show techniques to analyze the Round Trip Time. To measure the RTT, we adopt two methods to collect. One is round trip time measured by traceroute6. It sends UDP packets by IPv6 protocol, which payload length is 20 bytes with 40 bytes IPv6 header, controlling a "hop limit" field and attempts to elicit an ICMP6 TIME_EXCEEDED IN-TRANSIT and finally obtains an ICMP6 PORT UNREACHABLE response. This method measures the interval from sending packet to get ICMP6 PORT UNREACHABLE.

The other method is to measure polling interval from the time to send get request to the time to get response from the

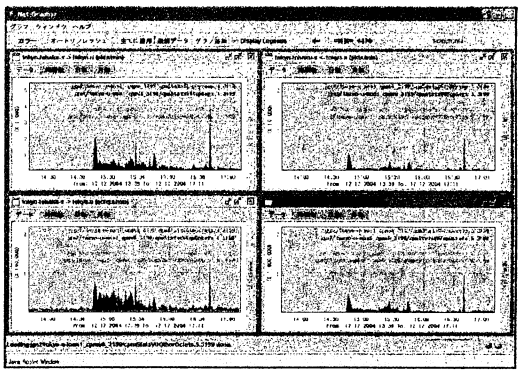

Fig. 3 Traffic Graph between RIEC in Tohoku University and the University of Tokyo

agent by SNMP over IPv6. We have been collecting these values every 60 seconds.

Firstly we consider about processing time. And next we survey the character of traceroute6 comparing and SNMP to collect traffic statistics with the mean and mode value of each statistics. Finally, as we collect these statistics from two different sites, we consider the correlation of these values.

4.1 Processing Time

Here we consider about processing time. We evaluate the RTTs measured by traceroute6 and SNMP to collect traffic statistics to the node on the same link (we call the later one "SNMP-RTT"). We might bypass influences by transit time from these measured values to do above.

We show these results on Fig 4. The measurement is done on 19th Nov. 2004. Remark that Y-axis scale is log-scale. There nodes in this experiment are on the same LAN. In the case of Kyoto, the source and target are on the same host.

The figure on left side shows the distribution of traceroute6's RTT and SNMP-RTT in Sendai. The figure on right side shows the distribution of traceroute6's RTT and SNMP-RTT in Kyoto. We also draw the line at the mode value for SNMP-RTT. But the mode values of traceroute6's RTT is are both 0 so we cannot draw those lines because Y-axis is log-scale. We can ensure that the processing time depends on the measurement tools.

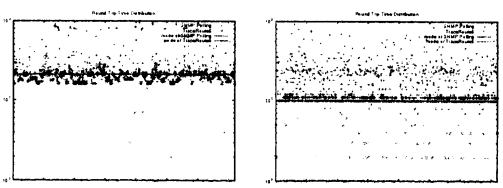

Fig. 4 traceroute6's RTT and SNMP-RTT to the node on the same LAN

4.2 Mode and Mean Properties

Here we discuss the statistics from RTT measurement. From Fig. 5 to Fig. 13 are graphs to plot the traceroute6's RTT and SNMP-RTT for each probes on 19th Nov. 2004. And also we draw the line at the value where the mean and mode value for the sets for each traceroute6's RTT and SNMP-RTT. Note that we did not have reachability for one probe on that day. Therefore, there are only 9 graphs. We can see from these figures that there are stability for time duration of traceroute and polling interval, and also, the difference between them is almost constant.

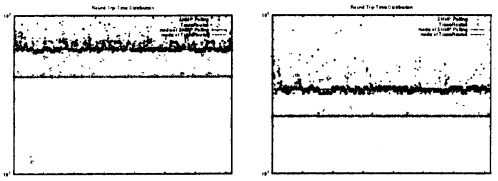

Fig. 5 Traceroute6's RTT ans SNMP-RTT for the node at Hiroshima City Univ.

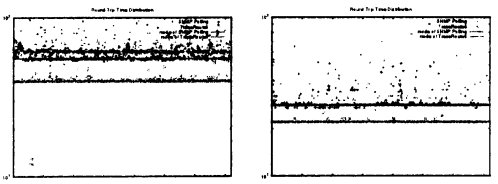

Fig. 6 Traceroute6's RTT ans SNMP-RTT the node at Hiroshima Univ.

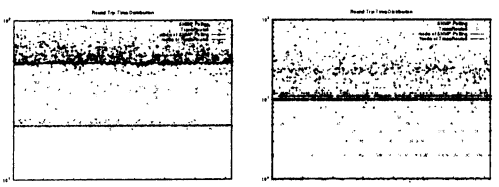

Fig. 7 Traceroute6's RTT ans SNMP-RTT for the node at Kyoto Univ.

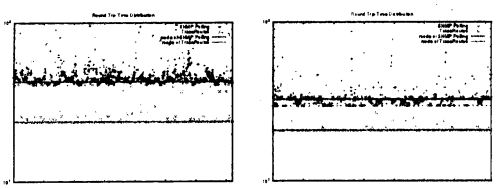

Fig. 8 Traceroute6's RTT ans SNMP-RTT for the node at Synergy Center in Tohoku Univ.

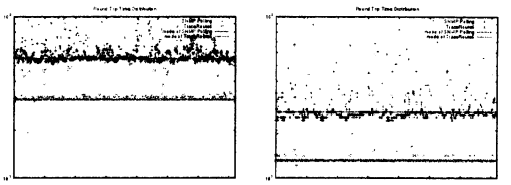

Fig. 9 Traceroute6's RTT ans SNMP-RTT for the node at Saga Univ.

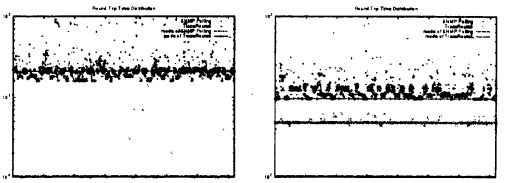

Fig. 10 Traceroute6's RTT ans SNMP-RTT for the node at Sendai (Cyber Solutions Inc.)

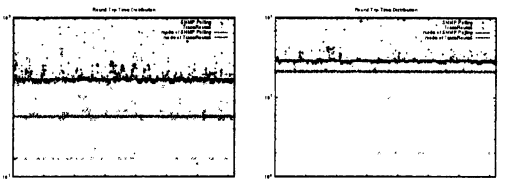

Fig. 11 Traceroute6's RTT ans SNMP-RTT for the node at RIEC in Tohoku Univ.

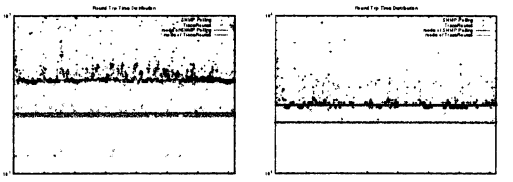

Fig. 12 Traceroute6's RTT ans SNMP-RTT for the node at TRIX

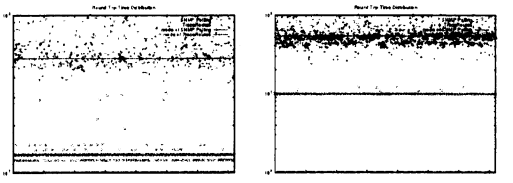

Fig. 13 Traceroute6's RTT ans SNMP-RTT at the Univ. of Tokyo

Next, we consider the daily distribution of traceroute6's RTT and SNMP-RTT. We focus on two statistics, the mean value and the mode value. The figure on the left side shows the daily distribution of RTTs from Sendai. The figure on the right side shows the daily distribution of RTTs from agents

at Kyoto University.

Fig. 20 shows the daily distribution of RTTs to Research Institute of Electrical Communication (RIEC) in Tohoku University. We can see from the figure that there are not so fluctuate in traceroute6's and SNMP–RTT. In contrast with this, Fig. 22 shows the same graph but the destination is a node located at the University of Tokyo. This figure shows the median value and mode value of traceroute6's RTT which are stable. but there is a variation in the values of SNMP–RTT from Sendai compared to the values from Kyoto. We can guess that there are some problems on the path between Sendai and the University of Tokyo. Also we can see from the graphs of Kyoto's agent that the mode values of traceroute6 on 8th Nov., 9th Nov., and 10th Nov. have the gap from the mean values of traceroute6.

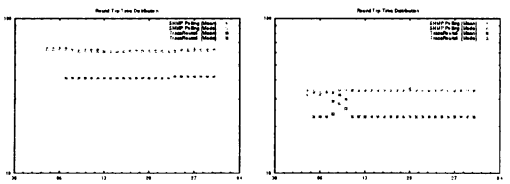

Fig. 14 Daily Distribution of traceroute6's RTT and SNMP–RTT in Hiroshima City Univ. on Nov. 2004

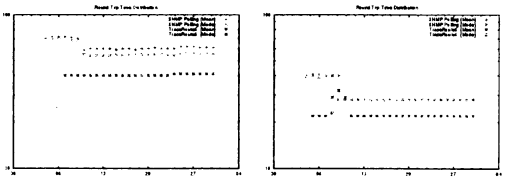

Fig. 15 Daily Distribution of traceroute6's RTT and SNMP–RTT in Hiroshima Univ. on Nov. 2004

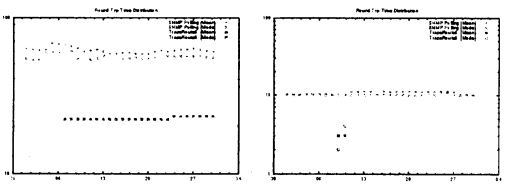

Fig. 16 Daily Distribution of traceroute6 RTT and SNMP–RTT in Kyoto Univ. on Nov. 2004

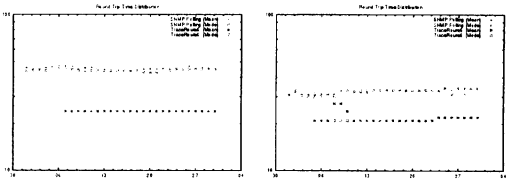

Fig. 17 Daily Distribution of traceroute6's RTT and SNMP–RTT in Synergy Center at Tohoku Univ. on Nov. 2004

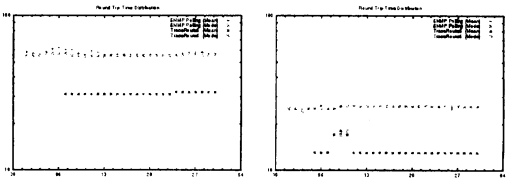

Fig. 18 Daily Distribution of traceroute6's RTT and SNMP–RTT in Saga Univ. on Nov. 2004

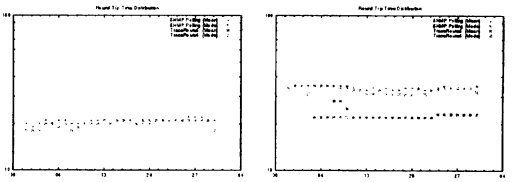

Fig. 19 Daily Distribution of traceroute6's RTT and SNMP–RTT in Sendai (Cyber Solutions Inc.)

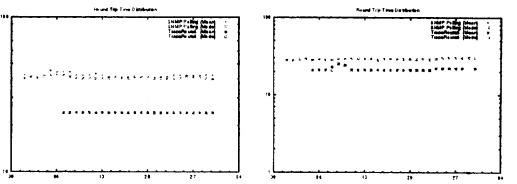

Fig. 20 Daily Distribution of traceroute6's RTT and SNMP–RTT in RIEC at Tohoku Univ. on Nov. 2004

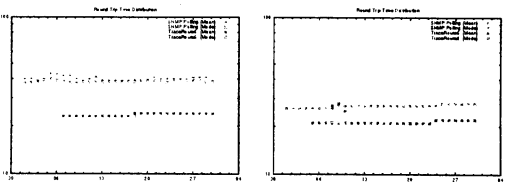

Fig. 21 Daily Distribution of traceroute6's RTT and SNMP–RTT in TRIX on Nov. 2004

4.3 Correlation

We have been monitoring network traffic statistics from two different sites. So we evaluate the correlation of traceroute6's RTT and SNMP–RTT.

Fig. 23 plots the RTT values where X–value is the value

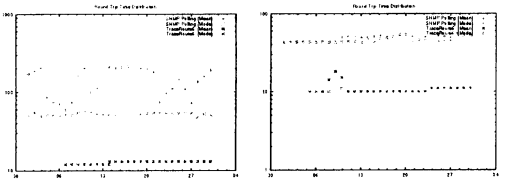

Fig. 22 Daily Distribution of traceroute6's RTT and SNMP–RTT to the probe at the University of Tokyo on Nov. 2004

from Sendai and Y–value is from Kyoto on 19th Nov. 2004. The drawing points of traceroute6's RTT are centered on one point, but the points of SNMP–RTT vary widely. The reason we can see the concentrated points on the line $X = 1,000$msec. and $Y = 1,000$msec, is because we set 1 second as retry interval for SNMP Polling.

Note that we did not have reachability for one probe on that day. We can also observe that the SNMP–RTT seen from Sendai is not stable in compared with the SNMP–RTT seen from Kyoto.

5. Conclusion

In this paper, we have focused on RTT as a statistics for estimating network performance and operational status. We have used "SNMP–RTT" values obtained as a by–product of network monitoring. We have analyzed the usefulness and significance of this statistics. We have shown that SNMP–RTT is useful in obtaining an insight into the operational dynamics of the network.

As future work, we introduce the reason we have been monitoring and analyzing network traffic. We are aiming at modeling network traffic statistics and we obtain hints to analysis deeply if measured traffic statistics is errant from established traffic model. We will make the model for RTT values in JGN–II network and discuss event detection with these statistics applying for network management. And we will continue further consideration to the properties of RTT values.

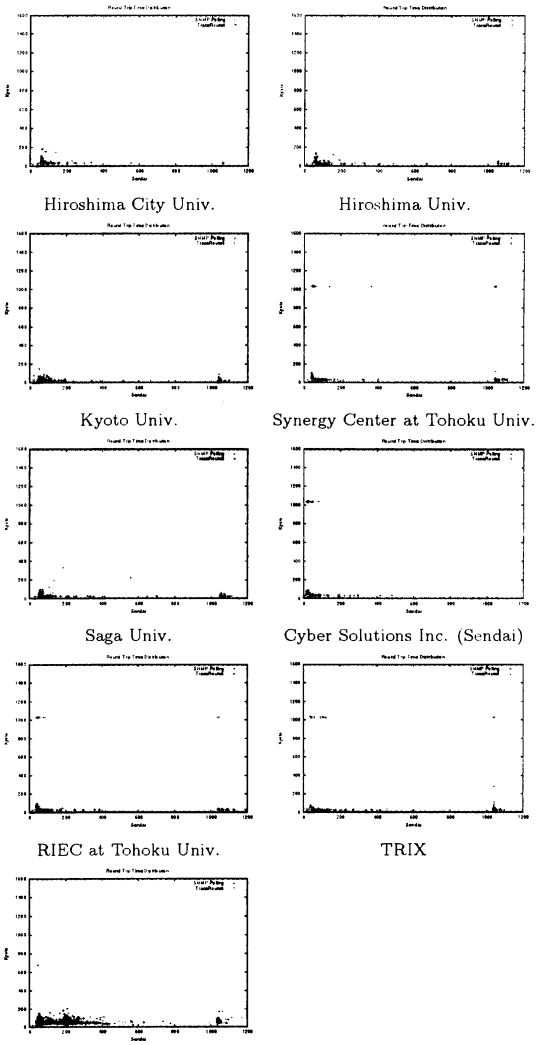

Fig. 23 Correlation of traceroute6's RTT and SNMP–RTT from two different sites

Reference

[1] "JGN II advanced network testbed for R & D offical website." http://www.jgn.nict.go.jp/.

[2] "JGN II Monitoring Project." http://www.cysol.co.jp/research/jgn2mon/.

[3] B. Huffaker, M. Fomenkov, D.J. Plummer, D. Moore, and k claffy, "Distance metrics in the internet," IEEE International Telecomunications Symposium (ITS2002), 2002.

[4] K. Abe, G. Mansfield Keeni and N. Shiratori, "Expreriments on Event Detection by Traffic Monitoring", TECHNICAL REPORT OF IEICE NS2004-89, IN2004-48, CS2004-44(2004-09), pp. 23–26, 2004.

[5] G. Mansfield Keeni, K. Koide, T. Saito and N. Shiratori, "Network Traffic Monitoring – the challenges", TECHNICAL REPORT OF IEICE IN2004-34 (2004-07), pp. 43–48, 2004.

[6] S. Floyd and V. Paxson, "Difficulties in Simulating the Internet", IEEE/ACM Transactions on Networking, Vol.9, No.4, pp. 392–403, 2001.

[7] V. Paxson and S. Floyd, "Wide-area Traffic: The Failure of Poisson Modeling", IEEE/ACM Transactions on Networking, Vol.3, No. 3, pp.226-244, 1995