Vol. 43 No. 11 IPSJ Journal Nov. 2002

Regular Paper

Inferring Traffic Flow Characteristics from Aggregated-flow Measurement

Masato Tsuru,[†1,†2] Tetsuya Takine[†3] and Yuji Oie[†1,†4]

In the Internet, a statistical perspective of global traffic flows has been considered as an important key to network operations and management. Nonetheless, it is expensive or sometime difficult to measure statistics of each flow directly. Therefore, it is of practical importance to infer unobservable statistical characteristics of individual flows from characteristics of the aggregated-flows, which are easily observed at some links (e.g., router interfaces) in the network. In this paper, we propose a new approach to such inference problems based on finding an inverse function from (observable) probabilities of some states on aggregated-flows to (unobservable) probabilities of some states on flows on a discrete state model, and provide a method inferring arrival rate statistics of individual flows (the OD traffic matrix inference). Our method is applicable to cases not covered by the existing normal-based methods for the OD traffic matrix inference. We also show simulation results on several flow topologies, which indicate potential of our approach.

1. Introduction

The Internet is currently shifting towards a social and economical infrastructure, which needs to be operated in a reliable and efficient way, and thus whose characteristics should be measurable. For example, a statistical perspective of global traffic flows has been considered as an important key to network operations and management, e.g., configuration, provisioning, traffic engineering, and detection of anomalous or malicious activities. Nonetheless, it is expensive or sometime difficult to measure statistics of each flow directly, i.e., based on identifying the flow to which each packet belongs by referencing the source and destination IP addresses in the packet and a global routing information at that time (although several researches tried it by capturing and analyzing raw traffic data in a network [1)]). Moreover, we need to treat cases in which source IP addresses are not reliable (e.g., watching malicious packets). Therefore, it is of practical importance to infer unobservable statistical characteristics of individual flows from characteristics of the aggregated-flows, which are easily observed at some links (e.g., router interfaces) in the network.

In this paper[☆], we propose a new approach to infer statistical characteristics of each flow from only observation of the aggregated-flows. We regard a "flow" as a series of (some kind of) packets from an origin node to a destination node under a fixed routing scheme. Here we intend that a "node" does not correspond to a single host but to a large set of hosts (i.e., a network or a set of networks), and thus a "flow" is not related to source-destination IP addresses directly but to a partial topological structure of routing paths in a network, e.g., routes from an Internet Service Provider (ISP) to another ISP.

Let us consider flows $f_1, f_2, \dots f_p$, and directed-links $l_1, l_2, \dots l_q$. Each link l_i is associated with a set F_i of flows where all (and only) flows in the set F_i pass through link l_i. The goal is to infer characteristics of each flow f_j ($1 \le j \le p$) from only observation of aggregated-flow F_i at link l_i ($1 \le i \le q$). We assume that we can observe all aggregated-flows $F_1, \dots F_q$ simultaneously so that we know correlations among them. Thus, if there exists an injection from each flow to a set of aggregated-flows including the flow (assuming $p \le 2^q - 1$), and if each flow behaves independently, we have a chance to infer some statistics on each flow from such correlations among a set of aggregated-flows.

The arrival rate, i.e., the number of arriving traffic bytes or packets in a unit time-interval, is a typical example of such flow characteristics. The inference of arrival rates of individual flows is known as the origin-destination (OD) traffic matrix problem. Originally, the OD traffic matrix problem is to infer unob-

†1 Telecommunications Advancement Organization of Japan
†2 Japan Telecom Information Service Co., Ltd.
†3 Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University
†4 Department of Computer Science and Electronics, Kyushu Institute of Technology

☆ A preliminary work of this paper was presented in IEEE/IPSJ SAINT2002 [2)].

servable OD flow traffic intensity (byte counts) from the link traffic intensity (byte counts) measured at some routers' interfaces, and several researches have studied this problem [3)~6)]. They assumed that all OD byte counts were modeled by independent normal distributions with a special relation between means and variances (or Poisson distributions), and were *iid* over successive measurement time-intervals or something like that. Then they employed the Expectation-Maximization (EM) algorithm to approximately calculate the maximum likelihood estimators (MLE) for the parameters of the models. However, since those methods were based on normal models, they were not applicable to irregular or small volume flows.

Our approach is different from the above approach. It is based on a principle proposed as a general framework of "inverse function approach" i.e., by finding a map from some (observable) resultant probabilities to some (unobservable) causal probabilities on a discrete model [7)], which is regarded as a generalization of a method inferring internal queuing delay statistics using end-to-end measurements of multicast probe packets [8)]. In accordance with the principle, we model the number of arriving packets in a measurement time-interval on each flow as an independent discrete random variable, and determine the distribution (i.e., histogram) consistent with observed data. Our method is applicable to flow rates with general (irregular) distributions that cannot be captured by normal-based models. On the other hand, our method requires that the number of arrivals in a measurement time-interval should sometimes take 0. In this paper, therefore, instead of inferring the rate of the whole traffic, we focus especially on inferring the arrival rate of some kind of special packets, where by "special" we mean that such packets do not always arise in each measurement interval. Of course, this condition is relative to the scale of measurement interval time, and thus a very short interval time may allow us to infer the rate statistics of the whole traffic. However, our intention is to infer statistics of some irregular events with a distribution that is not covered by the existing normal-based methods. For example, we intend to infer the rate statistics of some kind of ICMP packets, packets with some kind of IP options, or IPv6 packets. Other end-to-end events related to TCP or application layers can be dealt with by our method if routers count such events. It is expected that the dynamics of such special events on each flow indicate useful information on anomalous congestion, malicious activities, or deployment of some optional functions, for example.

The remainder of this paper is organized as follows. Section 2 describes a general model consisting of flows, links, aggregated-flows, and characteristics of flows to be inferred. Section 3 explains how to apply the inference principle to inferring arrival rates of packets with some examples. Section 4 shows simulation results. Finally Section 5 concludes this work.

2. General Model

We define a model for the inference problem based on a general framework [7)].

2.1 Links and Flows

Let us consider a directed-graph consisting of nodes (vertexes) and directed-links (edges), and flows on the graph. Each flow is a series of some kind of packets from an origin node to a destination node along a fixed sequence of directed-links without a loop. We call a set of flows passing through a link by an "aggregated-flow" passing through that link.

Link is defined as a set consisting of all observable links at which the characteristic of the aggregated-flow passing through the link can be obtained from observations. Typically, ***Link*** corresponds to a set of (incoming and/or outgoing) interfaces of one or more routers in a network. ***Flow*** is defined as a set consisting of all flows passing through at least one of links in ***Link***.

For each flow $e \in \boldsymbol{Flow}$, we define passing-link set $\boldsymbol{R}(e)$ as a set of links in ***Link*** that are passed through by the flow e. Note that $\boldsymbol{R}(e) \neq \emptyset$. We denote a set consisting of all passing-link sets by Δ: $\Delta \stackrel{\text{def}}{=} \{\boldsymbol{R}(e) | e \in \boldsymbol{Flow}\}$. Then, for $R \in \Delta$, we define "distinguishable flow" f_R as a set $\{e | \boldsymbol{R}(e) = R\}$ of flows. In other words, we label each (distinguishable) flow by its passing-link set R. We also denote a set consisting all "distinguishable flow"s by Δ^*. In what follows, we use a term "flow" as a "distinguishable flow".

For each link $l \in \boldsymbol{Link}$, we define $\boldsymbol{F}_l$ as a set of flows (an aggregated-flow) passing through link l: $\boldsymbol{F}_l \stackrel{\text{def}}{=} \{f_R | l \in R, R \in \Delta\}$. Without loss of generality, we assume that $\boldsymbol{F}_{l_1} \neq \boldsymbol{F}_{l_2}$ if $l_1 \neq l_2$.

Figure 1 shows four examples. Both (I) and

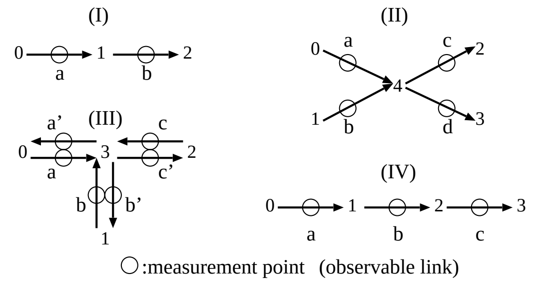

Fig. 1 Examples of the network model (nodes, links and flows).

Table 1 Links and flows in the examples.

	(I)	(II)	(III)	(IV)
Link	a, b	a,b,c,d	a,b,c,a',b',c'	a, b, c
Flow (Δ)	a, b, ab	ac, ad, bc, bd	ab', ac', a'b, bc', a'c, b'c	a, b, c, ab, bc, abc

(III) have three end nodes 0, 1, and 2, and both (II) and (IV) have four end nodes 0, 1, 2 and 3, where, by "end node", we mean an origin and/or destination node of a flow. Links and flows on them are shown in **Table 1**. In (I), $\boldsymbol{Link} = \{a, b\}$, and $\Delta = \{a, b, ab\}$, where f_a is a flow from node 0 to 1, f_b is from 1 to 2, and f_{ab} is from 0 to 2, respectively. Aggregated-flows are $\boldsymbol{F}_a = \{f_a, f_{ab}\}$ and $\boldsymbol{F}_b = \{f_b, f_{ab}\}$.

2.2 Characteristics of Flows to be Inferred

We define some notations to describe characteristics of a flow or a set of flows as follows.

- $\boldsymbol{M} = \{0, 1, \ldots M\}$: A set of integers representing states related to characteristic of a flow or a set of flows.
- $X_R(m)$: An unobservable event that the state of a flow f_R is $m \in \boldsymbol{M}$ for $R \in \Delta$.
- $V(F)(m)$: An event that the state of a set F of flows is $m \in \boldsymbol{M}$. If $F = \{f_R\}$ then $V(\{f_R\})(m) = X_R(m)$.
- $Y_l(m) \stackrel{\text{def}}{=} V(\boldsymbol{F}_l)(m)$: An observable event that the state of an aggregated-flow $\boldsymbol{F}_l$ is $m \in \boldsymbol{M}$ for $l \in \boldsymbol{Link}$.

We also define the occurrence probabilities related to the above events:

$$x_R(m) \stackrel{\text{def}}{=} \Pr[X_R(m)],$$

$$\underline{y}(R)(m) \stackrel{\text{def}}{=} \Pr[\bigcup_{k=0}^{m} \bigcup_{l \in R} Y_l(k)],$$

$$\overline{y}(R, R')(m) \stackrel{\text{def}}{=} \Pr[\bigcap_{l \in R \setminus R'} Y_l(0) \cap \bigcap_{l \in R'} Y_l(m)],$$

where $\underline{y}(R)(m)$ means, for a set R of links, the probability that the state of at least one aggregated-flow in the set $\{\boldsymbol{F}_l | l \in R\}$ is within $\{0, 1, \ldots m\}$; and $\overline{y}(R, R')(m)$ means, for two sets R and R' satisfying $R' \subset R$, the probability that the states of all aggregated-flows in the set $\{\boldsymbol{F}_l | l \in R - R'\}$ are the same 0, and the states of all aggregated-flows in the set $\{\boldsymbol{F}_l | l \in R'\}$ are the same m. We assume the following conditions on $\{V(F)(m) | F \subset \Delta^*, F \neq \emptyset, m \in \boldsymbol{M}\}$:

(i) States on a flow (or a set of flows) occur exclusively, i.e., $V(F)(i) \cap V(F)(j) \neq \emptyset$ if $i \neq j$.

(ii) States on different flows (or exclusive sets of flows) occur independently, i.e., $V(F)(i)$ and $V(F')(j)$ are independent if $F, F' \neq \emptyset$, $F \cap F' = \emptyset$, $i, j \in M$.

(iii) State 0 sometimes occurs, i.e., $0 < \Pr[V(F)(0)]$.

(iv) A certain technical condition holds on the relation between $V(F + F')(m)$ and $V(F)(s_1) \cap V(F')(s_2)$ for $\forall s_1, s_2 \leq m$. Note that if $V(F)(m)$ satisfies ($m \in \boldsymbol{M}$)

$$V(F + F')(m) = \sum_{j=0}^{m} V(F)(j) \cap V(F')(m - j) \qquad (1)$$

then it also satisfies this condition (iv).

Then, it can be shown that $\underline{y}(R)(m)$ and $\overline{y}(R, R')(m)$ can be calculated from $\{x_R(m)\}$, i.e., there exists map $\boldsymbol{G}$:

$$\left(\underline{y}(R)(m), \overline{y}(R', R'')(m)\right)_{R, R', R'', m} = \boldsymbol{G}(x_R(m); m \in \boldsymbol{M}, R \in \Delta)$$

Roughly speaking, the key of our inference principle is that we can find inverse map $\boldsymbol{G}_{R,m}^{-1}$ such that

$$x_R(m) = \boldsymbol{G}_{R,m}^{-1}(\underline{y}(.)(i), \overline{y}(.,.)(i); 0 \leq i \leq m)$$

by taking appropriate $\underline{y}(.)$ and $\overline{y}(.,.)$ according to $R \in \Delta$. In other words, if we can obtain the occurrence probabilities of some kinds of concurrent states on appropriate sets of aggregated-flows:

$$\{\underline{y}(R)(m), \overline{y}(R', R'')(m) | m \in \boldsymbol{M}, R \in \Psi, R' \in \Psi', R'' \text{ is a subset of } R'\},$$

where Ψ and Ψ' are appropriate subsets of $2^{\boldsymbol{Link}}$, then we can also obtain (determine) the occurrence probabilities of individual states on individual flows:

$$\{x_R(m) | 0 \leq m \leq M, R \in \Delta\}.$$

Note that this is the generic form, and in the next section, we introduce a more specific form for some example topologies.

3. Inference Method for Arrival Rates

3.1 Inference of Arrival Rates

We explain how to infer the distribution of each flow rate from observation of aggregated-flow rates. First, we should define the unit time for the "(arrival) rate". Let T (sec) be a unit time (i.e., the length of each measurement interval) for the rates so that a "flow rate" is defined as "the number of arriving packets on a flow in a T interval". To obtain the distribution (or statistics) of a rate, for a sufficient large n, we repeatedly measure the rate in n successive measurement intervals: $\{[(i-1)T, iT); i = 1, 2, \ldots n\}$. For each $i \in \{1, 2, \ldots n\}$, let w_i^l and v_i^R be the number of packets arriving to aggregated-flow $\boldsymbol{F}_l$ and flow f_R in the i-th measurement interval, respectively. The number of arrivals ranges from 0 to M. We assume that $\{v_i^R | 1 \leq i \leq n\}$ is regarded as *iid* for each R, and thus we can let v^R be a random variable behind the measurements that represents the number of packets arriving to flow f_R in a measurement interval. We ignore the problem of packet transmission delay and clock synchronization between different measurement points (e.g., router interfaces) so that we assume that w_i^l can be exactly observed at link l. Our goal is to infer the distribution of v^R:

$$x_R(m) \stackrel{\text{def}}{=} \Pr[v^R = m], \quad m \in \boldsymbol{M},$$

for each flow f_R, by which we can obtain the mean rate:

$$E[v^R] \stackrel{\text{def}}{=} \sum_{m=0}^{M} m x_R(m)$$

or the normalized mean rate $E[v^R]/T$.

We have the system (linear equations) among observable w_i^l and unobservable v_i^R for each $i \in \{1, 2, \ldots n\}$.

$$w_i^l = \sum_{f_R \in \boldsymbol{F}_l} v_i^R \quad \text{for } l \in \textbf{\textit{Link}} \qquad (2)$$

If the above Eq. (2) is uniquely solvable, then we have map $\boldsymbol{H}^R$ such that $v_i^R = \boldsymbol{H}^R(w_i^l; l \in \textbf{\textit{Link}})$, and thus, for a sufficient large n, we can directly estimate $x_R(m)$ as:

$$\hat{x}_R(m) \stackrel{\text{def}}{=} \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}(v_i^R = m) = \frac{1}{n} \sum_{i=1}^{n} \mathbf{1}(\boldsymbol{H}^R(w_i^l; l \in \textbf{\textit{Link}}) = m)$$

where $\mathbf{1}(.)$ denotes the indication function.

Hereafter, we consider cases in which Eq. (2) is not uniquely solvable. In such cases, although each v_i^R cannot be uniquely determined, we show that the distribution of v^R can be determined in a statistical way.

In accordance with the model in Section 2, since X_R should correspond to unobservable events on flow f_R and Y_l should correspond to observable events on aggregated-flow $\boldsymbol{F}_l$, let $V(F)(m)$ be event "$\sum_{f_R \in F} v^R = m$", $X_R(m)$ be event "$v^R = m$", and $Y_l(m)$ be event "$\sum_{f_R \in \boldsymbol{F}_l} v^R = m$", respectively, for $F \subset \Delta^*$, $R \in \Delta$, $l \in \textbf{\textit{Link}}$, and $m \in \boldsymbol{M}$.

Let us check the conditions on V in Section 2. Condition (i) is clear. Moreover we can show Eq. (1), so that condition (iv) is satisfied. Let F and F' be two exclusive sets of flows. In each measurement interval, it is clear that "the number of arriving packets on all flows in $F + F'$" = "the number of arriving packets on all flows in F" + "the number of arriving packets on all flows in F'". Hence, when $V(F+F')(m)$ occur, one of the following events must occur exclusively: $V(F)(0) \cap V(F')(m)$, ..., $V(F)(m-1) \cap V(F')(1)$, or $V(F)(m) \cap V(F')(0)$, which implies Eq. (1).

On the other hand, whether condition (ii) and (iii) are satisfied or not depends on both the nature of the target traffic and unit time T. Those conditions, therefore, are regarded as requirements (restrictions) for our approach. Note that (ii) is expected to be satisfied approximately because of diversity of traffic in actual networks.

3.2 Examples

While several estimators can be derived from the framework in the previous section, we can employ the most basic estimator on the binary-tree relation (the shared-part and two independent-parts) for the examples in this section. For concise descriptions, we prepare the following definitions of $\underline{x_R}(m)$, $y_l(m)$ and $y_{ll'}(m)$ for $R \in \Delta$, $m \in \boldsymbol{M}$, and $l, l' \in \textbf{\textit{Link}}$.

$$\underline{x_R}(m) \stackrel{\text{def}}{=} \Pr[v^R \leq m] = \sum_{k=0}^{m} x_R(k),$$

$$y_l(m) \stackrel{\text{def}}{=} \underline{y}(l)(m) = \Pr[\bigcup_{k=0}^{m} Y_l(k)],$$

$$y_{ll'}(m) \stackrel{\text{def}}{=} \underline{y}(l)(m) + \underline{y}(l')(m) - \underline{y}(ll')(m)$$

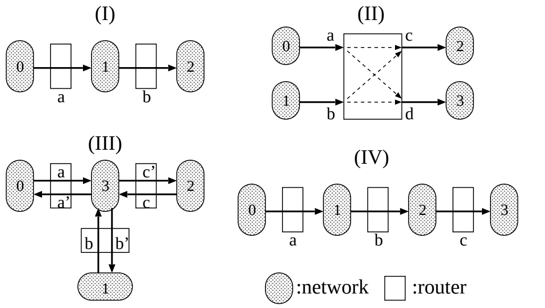

Fig. 2 Examples of flows on actual networks.

$$= \Pr[\bigcup_{k=0}^{m} Y_l(k) \cap \bigcup_{k=0}^{m} Y_{l'}(k)] \quad (3)$$

For a sufficient large n, we can directly estimate $y_l(m)$ and $y_{ll'}(m)$ as $\hat{y}_l(m)$ and $\hat{y}_{ll'}(m)$, respectively, by the sample means:

$$\hat{y}_l(m) \stackrel{\text{def}}{=} \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}(w_i^l \leq m),$$

$$\hat{y}_{ll'}(m) \stackrel{\text{def}}{=} \frac{1}{n}\sum_{i=1}^{n} \mathbf{1}(w_i^l \leq m \wedge w_i^{l'} \leq m) \quad (4)$$

In what follows, we show that we can find map $\boldsymbol{G}_{R,m}^{-1}$ (for each $R \in \Delta$ and each $m \in \boldsymbol{M}$) in examples in **Fig. 2**, by which we infer $x_R(m)$ as $\boldsymbol{G}_{R,m}^{-1}(\hat{y}_l(i), \hat{y}_{ll'}(i); l, l' \in \boldsymbol{Link}, 0 \leq i \leq m)$.

For (I) in Fig. 2 (modeled by (I) in Fig. 1), we observe aggregated-flows at two routers (interfaces) a and b, and can obtain (directly estimate), $\hat{y}_a(m)$, $\hat{y}_b(m)$, and $\hat{y}_{ab}(m)$, for $m \in \boldsymbol{M}$, from observed data $\{(w_i^a, w_i^b) | i = 1, 2, \ldots n\}$. The relation between unobservable flow rates (v_i^a, v_i^b, v_i^{ab}) and aggregated-flow rates (w_i^a, w_i^b) is shown by the following equation. **Figure 3** (I) also shows the relation.

$$\begin{pmatrix} w_i^a \\ w_i^b \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} v_i^a \\ v_i^b \\ v_i^{ab} \end{pmatrix}.$$

Since we assume that v^a, v^b, v^{ab} are independent each other (condition (ii) in the previous section), we have the following system $\boldsymbol{G}$ from Eq. (3).

$$y_a(m) = \sum_{i=0}^{m} x_{ab}(i)\underline{x_a}(m-i),$$

$$y_b(m) = \sum_{i=0}^{m} x_{ab}(i)\underline{x_b}(m-i),$$

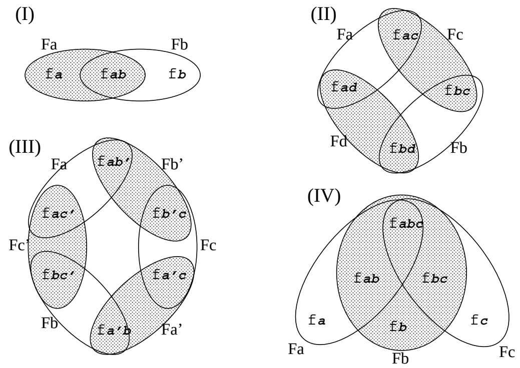

Fig. 3 Relation between flows and aggregated-flows.

$$y_{ab}(m) = \sum_{i=0}^{m} x_{ab}(i)\underline{x_a}(m-i)\underline{x_b}(m-i).$$

Then, since we assume that $0 < x_a(0)$, $x_b(0)$, $x_{ab}(0)$ (condition (iii) in the previous section), we can solve it inductively with respect to m as follows ($r \in \{a, b\}$):

$$\begin{aligned}
x_{ab}(0) &= \frac{y_a(0)y_b(0)}{y_{ab}(0)}, \\
\underline{x_a}(0) &= \frac{y_{ab}(0)}{y_b(0)}, \quad \underline{x_b}(0) = \frac{y_{ab}(0)}{y_a(0)}, \\
x_{ab}(m) &= \boldsymbol{G}_{ab,m}^{-1}(\boldsymbol{y_m}) \\
&\stackrel{\text{def}}{=} \frac{x_{ab}(0)}{2}\Big(E_{ab} - \\
&\quad \sqrt{E_{ab}^2 - \frac{4C_aC_b}{y_a(0)y_b(0)} + \frac{4D_{ab}}{y_{ab}(0)}}\Big), \\
\underline{x_r}(m) &= \frac{C_r - x_{ab}(m)\underline{x_r}(0)}{x_{ab}(0)}, \\
x_r(m) &= \boldsymbol{G}_{r,m}^{-1}(\boldsymbol{y_m}) \\
&\stackrel{\text{def}}{=} \underline{x_r}(m) - \underline{x_r}(m-1), \qquad (5)
\end{aligned}$$

where

$$\begin{aligned}
\boldsymbol{y_m} &\stackrel{\text{def}}{=} \{y_a(i), y_b(i), y_{ab}(i) | 0 \leq i \leq m\} \\
C_r &\stackrel{\text{def}}{=} y_r(m) - \sum_{i=1}^{m-1} x_{ab}(i)\underline{x_r}(m-i), \\
D_{ab} &\stackrel{\text{def}}{=} y_{ab}(m) - \\
&\quad \sum_{i=1}^{m-1} x_{ab}(i)\underline{x_a}(m-i)\underline{x_b}(m-i), \\
E_{ab} &\stackrel{\text{def}}{=} \frac{C_a}{y_a(0)} + \frac{C_b}{y_b(0)} - 1.
\end{aligned}$$

An intuition for the above identifiability is as follows. In a measurement interval, if we see no traffic at router a and some traffic at router

b, then we can know that the traffic belongs to flow b. This simple insight can be extended to a number of independent observations, and uniquely determines the statistics of flows a, b and ab consistent with the observed data. Note that, the smaller unit time T is used, the more chances to see no traffic at router a are expected, and thus, the more accurate inference can be done.

Note that another estimator for x_a and x_b can be derived from simple relations: $x_a(m) = \overline{y}(ab,a)(m)/y_b(0)$ and $x_b(m) = \overline{y}(ab,b)(m)/y_a(0)$, where $\overline{y}(R,R')(m)$ is defined in the previous section.

Hereafter we employ $x_.$ and $\hat{y}_.$ to denote $\{x_.(m)|m \in \boldsymbol{M}\}$ and $\{\hat{y}_.(m)|m \in \boldsymbol{M}\}$, respectively. For (II) in Fig. 2 (modeled by (II) in Fig. 1), we observe aggregated-flows at four interfaces a, b, c and d of a router, and can obtain, $\hat{y}_a$, $\hat{y}_b$, $\hat{y}_c$, $\hat{y}_d$, $\hat{y}_{ac}$, $\hat{y}_{ad}$, $\hat{y}_{bc}$, and $\hat{y}_{bd}$ by Eq. (4). Although the number of links is equal to the number of flows, Eq. (2) in this case is not uniquely solvable because of the implicit restriction $w_i^a + w_i^b = w_i^c + w_i^d$.

$$\begin{pmatrix} w_i^a \\ w_i^b \\ w_i^c \\ w_i^d \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} v_i^{ac} \\ v_i^{ad} \\ v_i^{bc} \\ v_i^{bd} \end{pmatrix}$$

In the same manner as the previous example, we can infer x_{ac} (from $\hat{y}_a$, $\hat{y}_c$ and $\hat{y}_{ac}$), x_{ad} (from $\hat{y}_a$, $\hat{y}_d$ and $\hat{y}_{ad}$), x_{bc} (from $\hat{y}_b$, $\hat{y}_c$ and $\hat{y}_{bc}$), and x_{bd} (from $\hat{y}_b$, $\hat{y}_d$ and $\hat{y}_{bd}$).

We show more realistic examples (III) and (IV). Figure 3 indicates that (III) is regarded as a straight-forward extension of (II). We observe aggregated-flows at three incoming interfaces (a, b, c) and three outgoing interfaces (a', b', c'), and then we infer $x_{ab'}$, $x_{ac'}$, $x_{a'b}$, $x_{bc'}$, $x_{a'c}$, and $x_{b'c}$.

For (IV) in Fig. 2, we observe aggregated-flows at only three routers a, b and c, and then we infer x_{abc}, $x_a x_{ab}$ and $x_c x_{bc}$ (from $\hat{y}_a$, $\hat{y}_c$ and $\hat{y}_{ac}$), $x_{ab}x_{abc}$, x_a, and $x_b x_{bc}$ (from $\hat{y}_a$, $\hat{y}_b$, and $\hat{y}_{ab}$), $x_{bc}x_{abc}$, x_c, and $x_b x_{ab}$ (from $\hat{y}_b$, $\hat{y}_c$ and $\hat{y}_{bc}$). Finally, we can infer each of x_{abc}, x_{ab}, x_{bc}, x_a, x_b, and x_c.

Before ending this section, we note that, computational cost of inferring all flow rate distributions is approximately $O(|\Delta| \times M^2 \times n)$, i.e., linear w.r.t. the number of flows, quadratic w.r.t. the number of discrete values, and linear w.r.t. the number of measurement intervals, which implies that M should be small in practical use. Therefore, in order to infer statistics of rates varying in a wide range, or rates as the number of arriving bytes (instead of arriving packets), we need to round (quantize) the number by an adequate bin size that depends on acceptable computational cost and required inference accuracy.

4. Simulation

We examine four examples shown in Fig. 2 through simulations. We dispatch a series of *ping*s, i.e., ICMP echo request 64-byte packets, as a target (to be inferred) flow. We employ three types of distributions of inter-arrival time between adjacent pings: (U) uniform distribution in a range $[0.2 \times m, 1.8 \times m]$ with mean m, (P) Pareto distribution with mean m and shape ρ, (E) exponential distribution with mean m. The bandwidth of each link is 1.5 Mb/s with 10 ms of propagation delay. We count the number of ICMP echo request packets arriving to each aggregated-flow in each measurement interval $[(i-1)T, iT)$ for $i = 1, 2, \ldots n$, where we choose 1 or 0.5 sec as unit interval time T. We infer, on each flow, the distribution of arrival rate of ping and then calculate the (normalized) mean arrival rate (the mean number of pings arriving in 1 sec).

For (I) of Fig. 2, we generate three independent streams of type-U ping with mean inter-arrival time $m = 1.5$ sec on flow f_a, a stream of type-E ping with $m = 0.4$ on f_{ab}, and a stream of type-P ping with $m = 0.3$ and $\rho = 1.5$ on f_b. Note that the theoretical mean rates (pps) are 2 for f_a, 2.5 for f_{ab}, and 3.3 for f_b, respectively.

To infer $x_r(m)$ for $r \in \{a, b, ab\}$, we need the division by $\hat{y}_r(0)$ in $\boldsymbol{G}^{-1}$ of Eq.(5). If one of $\hat{y}_a(0)$, $\hat{y}_b(0)$, and $\hat{y}_{ab}(0)$ is close to 0, the convergence of inferred value $\hat{x}_r(m)$ may be unstable because of a large relative error in $1/\hat{y}_r(0)$. Therefore, unit time T should be so small that the number of arrivals on each aggregated-flow in a measurement interval sometimes takes 0, i.e., $\hat{y}_r(0) \gg 0$. The top of **Fig. 4** shows the convergence of $\hat{y}_r(0)$ for $T = 1$ and 0.5 (sec). For $T = 1$, since $\hat{y}_{ab}(0)$ remains 0 until about 1,200 seconds elapse, $x_r(m)$ cannot be inferred by using $\boldsymbol{G}^{-1}$ there.

To see the relation between normalized mean arrival rate and the probability of no packet arriving in a T interval, let us consider the most simple case (i.e., all flows are the Poisson, so that all aggregated-flows are also the Poisson). If packets on an aggregated-flow has exponen-

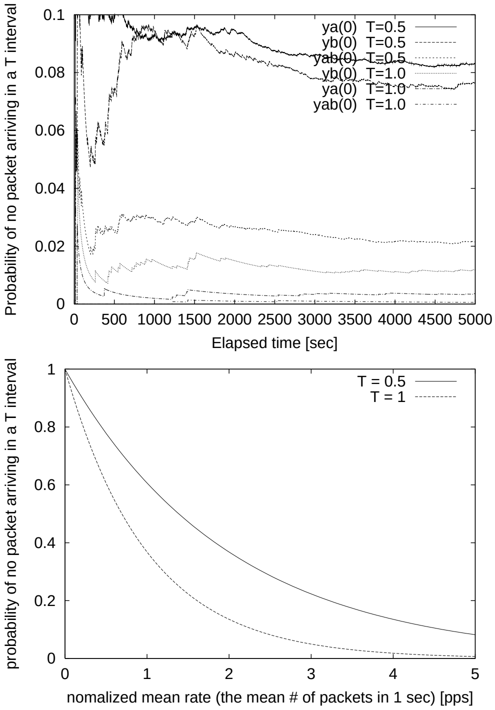

Fig. 4 Probability of no packet arriving in a T interval with $T = 1$ and $T = 0.5$ (sec).

Table 2 Flow parameters in a simulation for (II).

flow	pps	type	m	flow	pps	type	m
ac	2	U ×3	1.5	ad	1.4	P	0.7
bc	0.8	E	1.3	bd	3.3	E	0.3

tially distributed inter-arrival time with mean m, then normalized mean aggregated-flow rate is equal to $1/m$, and the probability of no packet arriving on the aggregated-flow in a T interval is equal to $\exp(-T/m)$. When the unit time decreases from T to T', the probability of no packet arriving in a unit time increases exponentially with respect to $(T - T')/m$. The bottom of Fig. 4 shows the relation between $1/m$ and $\exp(-T/m)$ for $T = 1$ or 0.5.

For (II), we generate three independent type-U streams on f_{ac}, a type-P stream ($\rho = 1.5$) on f_{ad}, a type-E stream on f_{bc}, and a type-E stream on f_{bd}, respectively, as shown in **Table 2**. For (III), we generate two independent type-U streams on $f_{ab'}$, a type-P stream ($\rho = 1.5$) on $f_{a'b}$, a type-E stream on $f_{bc'}$, two independent type-U streams on flow $f_{b'c}$, a type-P stream ($\rho = 1.3$) on $f_{a'c}$, and a type-E stream on $f_{ac'}$, respectively, as shown in **Table 3**. For (IV), we generate three independent type-U streams on flow f_a, two independent type-U streams on flow f_b, a type-P stream ($\rho = 1.5$) on f_c, a type-P stream ($\rho = 1.3$) on f_{ab}, a type-E stream on f_{bc}, and a type-E stream on f_{abc}, respectively, as shown in **Table 4**.

Table 3 Flow parameters in a simulation for (III).

flow	pps	type	m	flow	pps	type	m
ab'	0.6	U ×2	3.34	$a'b$	1.0	P	1.0
bc'	1.4	E	0.71	$b'c$	1.2	U ×2	1.67
$a'c$	2.0	P	0.5	ac'	2.8	E	0.36

Table 4 Flow parameters in a simulation for (IV).

flow	pps	type	m	flow	pps	type	m
a	1.2	U ×3	2.5	ab	0.7	P	1.5
b	0.8	U ×2	2.5	bc	0.8	E	1.3
c	1.3	P	0.8	abc	0.7	E	1.5

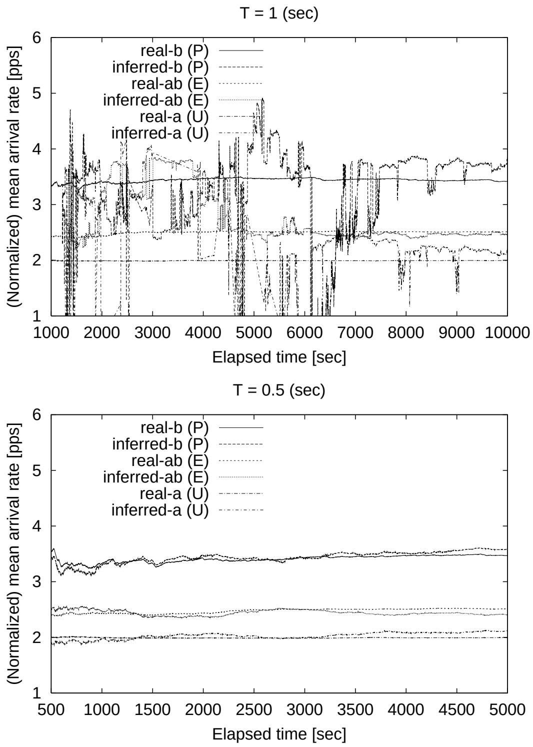

Fig. 5 The mean rates inference in (I) with $T = 1$ and $T = 0.5$.

Figure 5, **Fig. 6**, **Fig. 7**, **Fig. 8**, and **Fig. 9** show comparison between the real mean rates (denoted by "real-xx") and the inferred mean rates (denoted by "inferred-xx") on individual flows in duration $[0, t)$ where t is the elapsed time (sec) from the beginning of the measurement. Those figures correspond to case (I) with interval time $T = 1$ (sec) and 0.5, case (II) with $T = 1$ and 0.5, case (III) with $T = 1$ sec, case

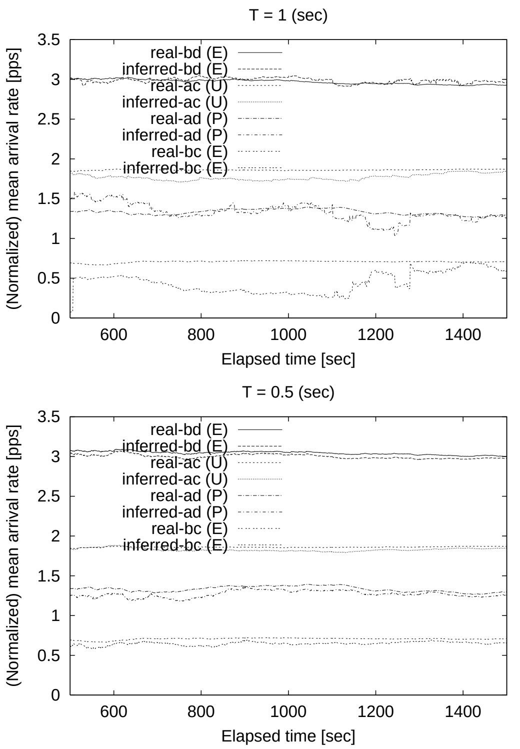

Fig. 6 The mean rates inference in (II) with $T = 1$ and 0.5.

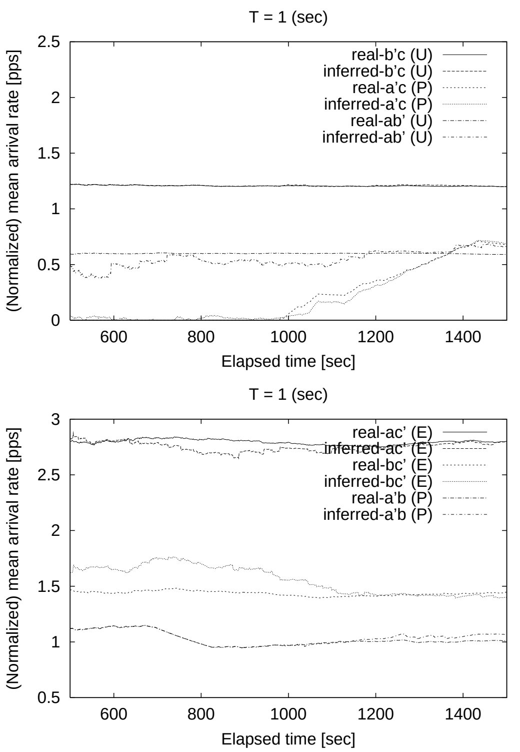

Fig. 7 The mean rates inference in (III) with $T = 1$.

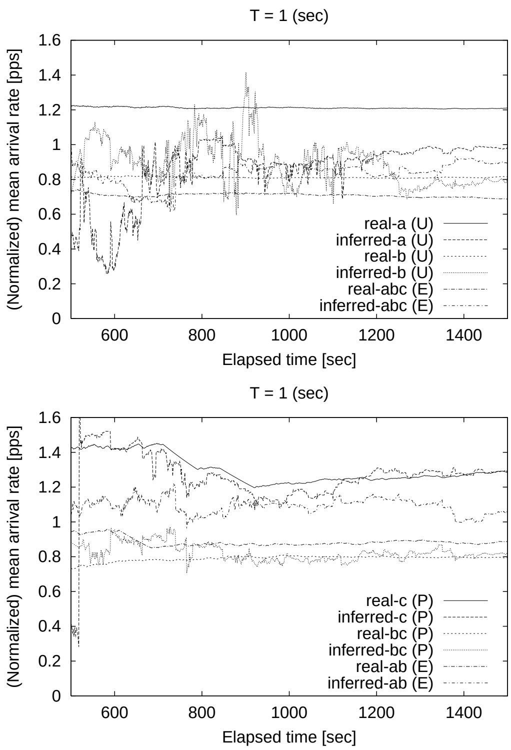

Fig. 8 The mean rates inference in (IV) with $T = 1$.

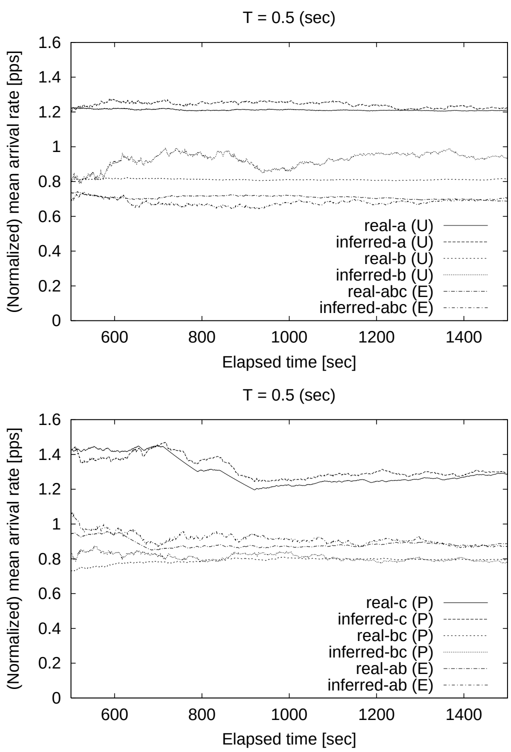

Fig. 9 The mean rates inference in (IV) with $T = 0.5$.

(IV) with $T = 1$, and case (IV) with $T = 0.5$, respectively.

The top of Fig. 5 shows a "bad" case in which the probabilities of no packet arriving on aggregated-flows in a measurement interval are very small (i.e., $y_a(0)$, $y_b(0)$, and $y_{ab}(0) \approx 0$) for $T = 1$, where we see very slow convergence. On the other hand, the bottom of Fig. 5 indicates a half measurement interval ($T = 0.5$) can dramatically increase those probabilities ($y_a(0)$, $y_b(0)$, and $y_{ab}(0) \gg 0$), and thus improve the convergence rates. This behavior is explained by Fig. 4 mentioned before.

In Fig. 6–Fig. 9, we can see acceptable convergences within 1,500 seconds under moderate conditions. Moreover, we do not see particular differences in inference accuracy among three types of distributions of the inter-arrival time. In cases (II) and (III), inference seems quite stable and accurate. On the other hand, in case (IV) with $T = 1$, although the inferred values roughly track the real values, we see a slow convergence with instability (Fig. 8), where we try to infer mean rates on six individual flows from observation of only three aggregated-flows. Case (IV) with $T = 0.5$ verifies that the shorter measurement interval time makes better stability and accuracy (Fig. 9).

5. Concluding Remarks

In this paper, we have presented a new approach to inferring unobservable statistical characteristics (occurrence probabilities of some discrete states) of individual flows from observable characteristics of some aggregated-flows. By this approach, the distribution of the number of packets (in a unit interval) arriving to each flow can be inferred by observing the number of packets arriving to the aggregated-flows at some links (e.g., interfaces of routers) over a number of unit intervals. Although our method requires some condition on dynamics of arrivals, it is applicable to general (irregular) distributions that cannot be captured by existing normal-based methods. For smaller mean rates and shorter measurement interval time, our model is expected to be more suitable. Note that we are studying how to relax such limitations. Furthermore, our method is computationally light-weight, which makes real-time estimations feasible. We have provided some examples and shown simulation results, which indicate potential of our approach.

For development and deployment of practical methods in actual networks based on our approach, we have many issues to examine and solve, such as, reliability and limitation (e.g., the acceptable degree of spatial / temporal dependence), distributed simultaneous measurements, and scalability. We should also further investigate statistical properties of our estimators, quantization techniques, collaboration with the MLE approach, and handling of time-varying nature (temporal dependence). In addition, our method may require additional functions to current routers in order to count some events in a short interval. However, this work has provided a starting point to establish a novel efficient inference of flow characteristics without identifying the flow to which each packet belongs.

References

1) Feldmann, A., Greenberg, A. G., Lund, C., Reingold, N., Rexford, J. and True, F.: Deriving traffic demands for operational IP networks: methodology and experience, *Proc. ACM SIGCOMM*, Stockholm, pp.257–270 (2000).

2) Tsuru, M., Takine, T. and Oie, Y.: Inferring traffic flow characteristics from aggregated-flow measurement, *Proc. IEEE/IPSJ SAINT*, Nara, Japan, pp.256–261 (2002).

3) Vanderbei, R. J. and Iannone, J.: An EM Approach to OD Matrix Estimation, SOR 94-04, Princeton Univ. (1994).

4) Vardi, Y.: Network tomography: Estimating source-destination traffic intensities from link data, *J. Am. Stat. Assoc.*, Vol.91, No.433, pp.365–377 (1996).

5) Tebaldi, C. and West, M.: Bayesian inference on network traffic using link count data, *J. Am. Stat. Assoc.*, Vol.93, No.442, pp.557–576 (1998).

6) Cao, J., Davis, D., Wiel, S. V. and Yu, B.: Time-Varying Network Tomography: Router Link Data, *J. Am. Stat. Assoc.*, Vol.95, No.452, pp.1063–1075 (2000).

7) Tsuru, M., Takine, T. and Oie, Y.: Inferring link characteristics from end-to-end path measurements, *Proc. IEEE ICC*, Helsinki, pp.1534–1538 (2001).

8) Presti, F. L., Duffield, N., Horowitz, J. and Towsley, D.: Multicast-based inference of network-internal delay distributions, TR 99-55, UMass Computer Science (1999).

(Received September 2, 2002)
(Accepted September 5, 2002)

Masato Tsuru received B.E. and M.E. degrees from Kyoto University, Japan in 1983 and 1985, respectively, and received D.E. degree from Kyushu Institute of Technology, Japan in 2002. From 1985 to 1990, he worked at Oki Electric Industry Co., Ltd., Tokyo. From 1990 to 2000, he was with the Information Science Center, Nagasaki University, Nagasaki. Since April 2000, he has been working at Japan Telecom Information Service Co., Ltd., and Telecommunications Advancement Organization of Japan, Kitakyushu. His research interests include performance measurement, modeling and analysis of computer communication networks. He is a member of the IPSJ, IEICE and JSSST.

Tetsuya Takine was born in Kyoto, Japan, on November 28, 1961. He received B.Eng., M.Eng. and Dr.Eng. degrees in applied mathematics and physics from Kyoto University, Kyoto, Japan, in 1984, 1986 and 1989, respectively. In April 1989, he joined the Department of Applied Mathematics and Physics, Faculty of Engineering, Kyoto University, as an Assistant Professor. Beginning in November 1991, he spent one year at the Department of Information and Computer Science, University of California, Irvine, on leave of absence from Kyoto University. In April 1994, he joined the Department of Information Systems Engineering, Faculty of Engineering, Osaka University as a Lecturer, and from December 1994 to March 1998, he was an Associate Professor in the same department. Since April 1998, he has been an Associate Professor in the Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University. His research interests include queueing theory and performance analysis of computer/communication systems. Dr. Takine is a fellow of the Operations Research Society of Japan, a member of the Institute of Electronics, Information and Communication Engineers of Japan, the Information Processing Society of Japan, the Institute of Systems, Control and Information Engineers, and IEEE. He received the Best Paper Award from the Operations Research Society of Japan in 1997.

Yuji Oie received B.E., M.E. and D.E. degrees from Kyoto University, Kyoto, Japan in 1978, 1980 and 1987, respectively. From 1980 to 1983, he worked at Nippon Denso Company Ltd., Kariya. From 1983 to 1990, he was with the Department of Electrical Engineering, Sasebo College of Technology, Sasebo. From 1990 to 1995, he was an Associate Professor in the Department of Computer Science and Electronics, Faculty of Computer Science and Systems Engineering, Kyushu Institute of Technology, Iizuka. From 1995 to 1997, he was a Professor in the Information Technology Center, Nara Institute of Science and Technology. Since April 1997, he has been a Professor in the Department of Computer Science and Electronics, Faculty of Computer Science and Systems Engineering, Kyushu Institute of Technology. His research interests include performance evaluation of computer communication networks, high speed networks, and queueing systems. He is a member of the IEEE, IPSJ, and IEICE.