Measurement Based Characterization of IP VPNs

Satish Raghunath, K.K. Ramakrishnan, Shivkumar Kalyanaraman

***Abstract*— Virtual Private Networks provide secure and reliable communication between customer sites. With the increase in number and size of VPNs, providers need efficient provisioning techniques that adapt to customer demand by leveraging a good understanding of VPN properties.**

In this paper we analyze two important properties of VPNs that impact provisioning - (a) structure of customer endpoint (CE) interactions and (b) temporal characteristics of CE-CE traffic. We deduce these properties by computing traffic matrices from SNMP measurements. We find that existing traffic matrix estimation techniques are not readily applicable to the VPN scenario due to the scale of the problem and limited measurement information. We begin by formulating a scalable technique that makes the most out of existing measurement information and provides good estimates for common VPN structures. We then use this technique to analyze SNMP measurement information from a large IP VPN service provider.

We find that even with limited measurement information (no per-VPN data for the core) we can estimate traffic matrices for a significant fraction of VPNs, namely, those constituting the "Hub-and-Spoke" category. In addition, the ability to infer the structure of VPNs holds special significance for provisioning tasks arising from topology changes, link failures and maintenance. We are able to provide a classification of VPNs by structure and identify CEs that act as hubs of communication and hence require prioritized treatment during restoration and provisioning.

***Index Terms*— VPN, Provisioning, Traffic Engineering, Traffic Matrix Estimation**

I. Introduction

Virtual Private Networks (VPNs) serve as a popular mechanism to provide secure connectivity among customer sites [2]. With increasing popularity of IP VPNs for enterprise networking solutions, providers are faced with new challenges in provisioning and operating a complex and growing VPN infrastructure.

In the presence of accurate information about customer traffic profile and available network resources, a provider can make accurate provisioning decisions while ensuring Service Level Agreements (SLAs) are met. However, in reality it is hard to specify customer traffic statistics accurately *a priori*. Existing architectures (e.g., the Hose Model [3], the Point-to-Set model [4], [5]) for scalable VPN services rely on adaptive provisioning strategies that require a good understanding of VPN characteristics, to avoid provisioning for peak demands. These models deliver multiplexing gain by leveraging the fact that traffic between VPN endpoints is often not meshed.

Our goal is to develop techniques that allow a service provider to learn properties of VPNs that impact provisioning tasks. We begin with SNMP measurement information from a large IP VPN service provider. For bandwidth allocation and resizing, we need temporal characteristics of traffic exchanged between pairs of customer endpoints (CEs). Provisioning tasks involving maintenance, recovery from link failures, topology changes, and re-homing customers are better accomplished if we can prioritize them for the hubs of communication in the VPN. Recent simulation studies [6] demonstrate this significance of VPN structure in provisioning. Thus, a good understanding of the structure of VPN endpoint interactions is required. Traffic engineering tasks involving core network capacity management require good estimates of the sizes of customer traffic aggregates, which can be derived from a knowledge of CE interactions, such as the CE-CE traffic matrix.

Recent advances in traffic matrix estimation techniques [7] provide a starting point. There are important differences in the VPN case that prevent us from directly employing existing traffic matrix estimation techniques: (a) the scale of the network taken as a whole results in a computationally expensive and infeasible formulation (e.g., 2.8×10^6 non-zero elements in a $(18 \times 10^3, 950 \times 10^3)$ sparse matrix in our case); (b) per-VPN traffic information is not available for core network links resulting in a lack of sufficient measurement information; (c) a shared core network infrastructure with only aggregate traffic counts for core network links introduces dependencies among the many VPNs that share those links.

Each of these issues assumes significance when we observe that with continual growth in the number of VPN customers, the scale of the problem increases. Obtaining fine-grained reliable measurement information becomes much harder. Thus we first evolve a scalable technique to compute VPN traffic matrices and then examine how to deal with the lack of sufficient measurement information. Specifically, we examine what characteristics of VPNs can be reliably estimated with existing information. In doing so, we are able to provide deployable techniques for improving the existing provisioning infrastructure. Additionally, our observations can serve as a guide to enhancement of existing measurement infrastructure for maximal gains.

We begin with an estimation technique that employs approximations to break the network-wide traffic matrix problem into several smaller independent per-VPN traffic matrix problems. These approximations are driven by exploiting distinct properties of VPNs. We demonstrate that despite insufficient information, we can learn VPN characteristics discussed above for a large fraction of customers.

Applying the estimation technique to the measurement information leads to the following significant contributions.

Besides confirming the intuition that Hub/Spoke VPNs are the most common kind, we find that mere traffic volume

S. Raghunath is with Juniper Networks, E-mail: rsatish@alum.rpi.edu

K.K. Ramakrishnan is with AT&T Labs - Research

S. Kalyanaraman is with Rensselaer Polytechnic Institute

Parts of this paper appeared in the IMC 2004 conference [1]. This work was funded by AT&T Labs Research and DARPA NMS contract F30602-00-2-0537.

SNMP Information	CE-PE and PE-PE traffic
SNMP Aggregation Interval	CE-PE-15m; PE-PE-1hr
VPN Size Range	10s to 100s CEs
Number of PE-PE Links	≈ 6000
Duration of data examined	5 months

TABLE I
DETAILS OF SNMP INFORMATION

measurements for the access link to a hub site or the contracted bandwidth (Committed or Peak Information Rates) are not enough to identify a site as a hub. We evolve thresholding techniques that leverage traffic matrices to characterize a site as a hub. We employ synthetic and measurement-based validation to understand the limitations of the estimation technique in the face of imperfect information.

First, we find that VPNs that exhibit a Hub/Spoke structure can be efficiently handled. Such VPNs feature many "spoke" nodes that communicate with just the "hub" nodes (typically one or two). We then employ traffic matrix estimates to obtain a classification of VPNs by their structure and show that Multi-hub/Spoke VPNs indeed constitute a significant fraction. We present analysis of Multi-hub/Spoke VPNs to show that many of them in fact feature two hubs as part of a dual-homed site. For the SNMP data analyzed in this paper, we show that traffic matrices can be accurately computed for a significant percentage (about 57%) of the VPNs.

Exploiting the higher accuracy in estimates of traffic matrices for Hub/Spoke VPNs, we then study temporal characteristics that affect bandwidth allocation tasks. We observe stable CE-CE traffic trends across weeks, and slowly varying trends across months. This lends support to bandwidth allocation strategies that might attempt to learn characteristics over time.

The combination of algorithms and measurement observations we present demonstrates the feasibility of adaptive provisioning. Despite the limited nature of available measurement information, we demonstrate that our techniques can be applied to a significant fraction of VPN customers implying an overall enhanced operational efficiency.

The rest of the paper is structured as follows. We discuss related work in §II. §III describes measurement information. A traffic matrix estimation technique is presented in §IV. Using synthetic inputs and SNMP data we validate the efficacy of the estimation technique in §V and §VI. We employ the technique to understand VPN structure and temporal characteristics in §VII and §VIII. We conclude in §IX.

II. RELATED WORK

A traffic matrix provides the volume of traffic between source-destination pairs in a network. Such matrices have been computed at varying levels of detail for IP networks: between ISP Points-of-Presence (PoPs) [8], routers [7], IP prefixes [9], using indirect tomographic techniques [10], [11], [12] etc. The problem of estimating traffic matrices can be highly under-constrained: for a network with N source-destination pairs we need N^2 demands to be estimated. However the number of pieces of information available is typically much smaller (of the order of number of links in the network). For large N, the problem becomes massively under-constrained. Such problems have been solved in many fields of engineering and science: seismology, astronomy, geophysics etc. [13], [14], [15] Existing research indicates that some kind of *side information* must be brought in while solving such linear systems in the form of an additional term in the optimization objective. Such a *regularization strategy* guides the optimization problem in its choice of the traffic matrix that might provide a good solution to the problem [16].

Zhang et al [7] develop a regularization method tailored for traffic matrix estimation. Their method incorporates the gravity model solution so that the optimization simultaneously attempts to minimize the error from observed link counts and the gravity estimate. They demonstrate that the gravity model estimate for the traffic matrix provides a good starting point and hence propose to opt for the Kullback-Leibler divergence of the gravity estimate from the variables being estimated as the regularization functional (§IV-A).

The problem treated here is closest to [7] in that, we adopt the same regularization technique. However, compared to the Border Router (BR) traffic matrix obtained in [7], the scale of the VPN problem is much larger. The computational expense prevents us from solving for a single network-wide problem (which is the case with BR traffic matrices). Instead we evolve approximation techniques that exploit the structure of VPNs and break the problem down to many per-VPN problems. In addition to problems with scale, the measurement information available with VPNs is aggregated across all VPNs and per-VPN information is very often unavailable (in contrast, the BR traffic matrices can exploit fine-grained NetFlow data). Hence it is not straightforward to gauge the correctness of the traffic matrix estimates in the case of VPNs. We evolve a set of guidelines to help understand the applicability of the estimates and demonstrate how to obtain the most out of the coarse-grain information available in the case of VPNs, inspite of the prohibitive scale of the problem.

Our work complements recent theoretical advances in designing optimal reservation trees for provisioning VPNs [17], [18], [19], [20]. Algorithms for computing reservation trees can benefit from up-to-date estimates for pair-wise bandwidth requirements for nodes in a VPN. Simulation studies [6] indicate that there can be significant benefits in incorporating traffic matrix information as a consequence of structural properties of VPNs.

III. MEASUREMENT INFORMATION

In this paper, we present results from our study of measurement information from a large VPN service. Here, we provide a brief description of the data available from the service. In addition to helping us understand the results in the next few sections, this is also meant to be representative of the kind of information that is typically at the disposal of today's service providers.

Fig. 1 shows the points in the network where SNMP measurement information is available. Aggregate byte counts over one hour intervals for each provider edge (PE) to PE link are collected by SNMP (Table I). This count represents the number of bytes transmitted on the PE-PE link due to *all*

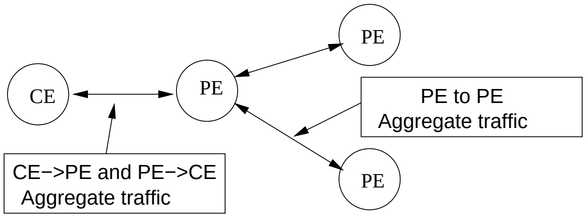


Fig. 1. Schematic showing available SNMP measurement information

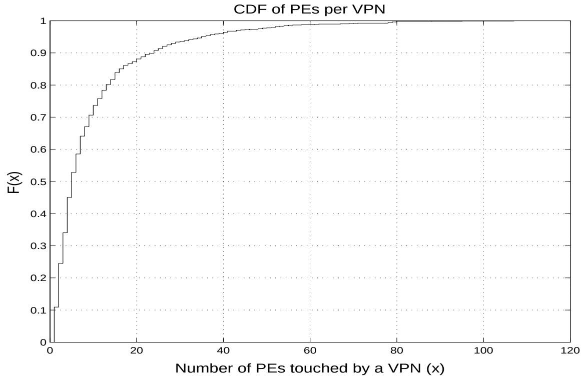


Fig. 2. CDF of number of PEs touched by a VPN

VPN customers sharing that link. By PE-PE link, we mean a logical link like an MPLS tunnel. In the current dataset there was SNMP information for such logical links for every pair of PEs. The other set of SNMP data available is for the traffic for each customer endpoint (CE) to PE link in the form of aggregate byte counts over 15 minute intervals. The CE-PE link is the dedicated access link for the VPN customer and the traffic observed on that link is due only to that CE.

As one would expect, the SNMP characteristics demonstrate weekly and daily cycles. As noted in [1], there is a mean about which the variations of traffic magnitude are seen, indicating that there is a certain amount of predictability in the traffic. We see stable trends in time-of-day variations across the multiple weeks of data examined

An important factor influencing our approach is the size of the service in terms of the number and size of customers, the number of PE routers involved and hence the scale of the problem. Fig. 2 shows the distribution of number of PEs that receive traffic per VPN. This measure indicates the number of links that traffic from a given VPN might influence. If there are N PEs that the CEs of a VPN communicate with, there can be $O(N^2)$ PE-PE paths that have to be factored in the estimation formulation. These PE-PE paths also carry traffic from other VPNs. Similarly the size of the VPN customers is an important measure of the scale of the problem. Fig. 3 gives the distribution of number of endpoints per VPN. The distribution shows that while there are a lot of small VPNs, there is a significant fraction with sizes in the tens and hundreds. In the absence of per-VPN traffic information on a per-link basis (as is the case here - the traffic counts for PE-PE logical links are aggregated across VPNs), the estimation has to account for all pairs of CEs as potentially communicating peers. The gist of these observations is that the scale of the problem at hand is considerable.

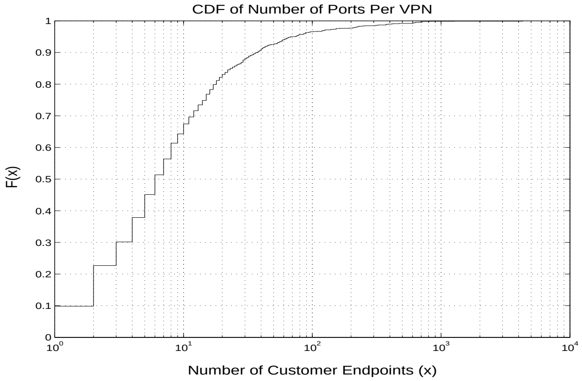


Fig. 3. CDF of number of CEs per VPN

IV. Traffic Matrix Estimation and Classification

There are multiple uncertainties to overcome while provisioning the network for the aggregate capacity needed for the VPN service. Some of the factors a carrier may not know precisely, a-priori, are:

- The amount of traffic generated by any given source of the VPN. We may only have the peak rate specification available.
- The proportion of the source (hose) traffic received by any given link in the network.

Often, a new VPN may be admitted with very little information being provided by the customer other than peak access capacity requirements. To guarantee the SLAs requested, there is a need to ensure that adequate resources are available. Understanding the “structure” of the VPN helps us to more efficiently provision the capacity in the network, and adapt the capacity to changing VPN requirements. By structure, we mean the spatial distribution of the traffic flows between the different sources and destinations of the VPN. For example, knowing if there is a hub-and-spoke structure helps in appropriately provisioning capacity in the network since an endpoint that is a spoke in a pure “hub-and-spoke” VPN would require capacity primarily between it and the hub. Provisioning without knowledge of the VPN structure could result in a substantial amount of wasted resources.

To infer the structure of a VPN and to achieve efficiencies through adaptive provisioning, we need to examine the way customer endpoints communicate with each other. In other words, we need good estimates of the VPN traffic matrix.

A. *Estimation techniques*

Inferring traffic matrices from link measurements can be highly under-constrained: with N nodes in a network, the number of traffic demands to be estimated is N^2 while the number of equations we have is only proportional to the number of links. As discussed in §II there are several approaches to solving such under-constrained problems. Two popular approaches are the gravity model approach and the information theoretic approach. We employ both.

Denote the total traffic from the network to an endpoint s_i by $N^{in}(s_i)$ and the traffic from that endpoint into the network by $N^{out}(s_i)$. Each element of the traffic matrix indicates the amount of traffic from source s_i towards destination d_j, denoted by $N(s_i, d_j)$. The gravity model attributes a portion of $N^{in}(d_j)$ received by d_j from each source s_i in proportion to the size of $N^{out}(s_i)$. The underlying assumption is that the amount of traffic generated by s_i is independent of that generated by d_j. Thus the following relationship is used: [7]

$$N(s_i, d_j) = \frac{N^{out}(s_i) N^{in}(d_j)}{\sum_{k \neq j} N^{out}(s_k)} \tag{1}$$

While the gravity model is simple, it is known to be less accurate in the presence of additional information. One of the methods recently proposed [7] exploits what is generally termed *strategies for regularization of ill-posed problems*. Accordingly**,** a penalized least-squares approach is formulated as:

$$min_x \left\{ ||\mathbf{y} - A\mathbf{x}||^2 + \lambda^2 \sum_{k:g_k>0} \frac{x_k}{T} log \left(\frac{x_k}{g_k} \right) \right\} \tag{2}$$

Here, $\mathbf{x}$ is a vector of elements x_k, such that for each variable $N(s_i, d_j)$, there exists an unique x_k representing it, with the constraint that $x_k \geq 0$. Each element y_k in vector $\mathbf{y}$ represents the traffic measured for link k, T is the total traffic in the network, and g_k is the gravity estimate for x_k obtained using Equation (1). A is the routing matrix which relates variables x_k appropriately - for each x_k representing $N(s_i, d_j)$, $A(l, k) = 1$ if traffic from s_i to d_j traverses the link y_l.

In the present context, s_i and d_j would correspond to the VPN customer endpoints. The set of variables $N(s_i, d_j)$ would be defined for each (s_i, d_j) that are part of the same VPN, since an endpoint communicates with another endpoint only if it is a part of the same VPN. Enumerating the constraints for all VPNs in the network would give us the equations denoted by Equation (2). Thus the following would be the set of equations forming the system:

1) $N^{out}(s_i) = \sum_j N(s_i, d_j)$, for each source s_i
2) $N^{in}(d_j) = \sum_i N(s_i, d_j)$, for each destination d_j
3) $N(PE_{kl}) = \sum_{\{(i,j) \in \Pi_k\}} N(s_i, d_j)$, for each PE-PE link PE_{kl} connecting PEs k and l, where the set Π_k contains (i, j) for every s_i routed to d_j through the link PE_{kl}

In reality, the problem described in Equation (2) is too big and computationally expensive to solve. For instance, for the measurement data analyzed here, we have a sparse routing matrix (A in Equation (2)) of dimensions $(18 \times 10^3, 950 \times 10^3)$ approximately, with about 2.8×10^6 non-zero elements. In this paper, we evolve a variant of the above estimation techniques to reduce the size of the problem so that the traffic matrices can be quickly computed.

B. Estimation of VPN Traffic Matrices

Although many VPNs share a common core network, no two endpoints belonging to different VPNs communicate with each other. This lends a kind of separability to our problem and hints at a possible strategy to reduce its size. Instead of solving the problem for all VPNs as part of a single network, we propose to compute the traffic matrices for each VPN independently. In order to do this, we need data on a per-VPN basis to construct the problem as in Equation (2). The path from a CE to another CE consists of two segments: a) an access segment (between the PE and the CE) where there is traffic from this VPN alone, b) a core network segment (link between two PEs) which carries traffic multiplexed across multiple VPNs. Typically, we have aggregate SNMP information for each of these segments. Thus we need to infer what part of the PE-PE aggregate traffic is attributable to the VPN being solved for, at each step. But there is not enough information to deduce this quantity. Instead, we introduce a bound on the contribution of a particular VPN to the measured PE-PE link traffic.

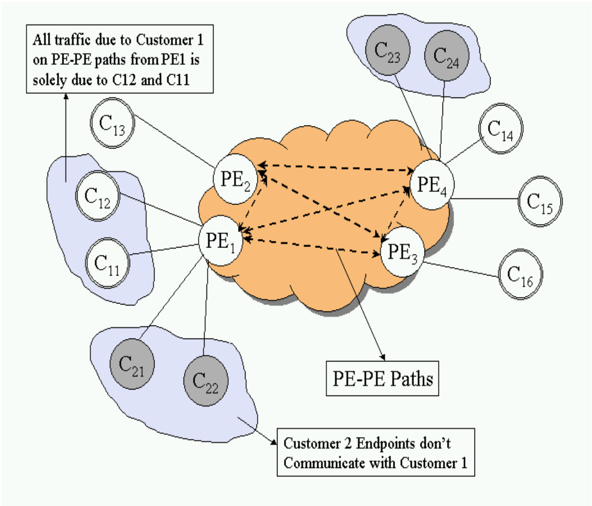

All traffic due to Customer 1 on PE-PE paths from PE1 is solely due to C12 and C11
C_{23}
C_{24}
C_{13}
C_{14}
PE_2
PE_4
C_{12}
C_{15}
PE_1
PE_3
C_{11}
C_{16}
C_{21}
C_{22}
PE-PE Paths
Customer 2 Endpoints don't Communicate with Customer 1

Fig. 4. Schematic indicating the structural aspects of VPNs that lead to additional equations in the Traffic Matrix estimation problem

Fig. 4 depicts the constraints we arrive at, by exploiting the structure of VPNs. We consider the set of all CEs in the VPN that can possibly transmit along a given PE-PE link. For example, in Figure 4 for the PE1-to-PE3 link, C_{11} and C_{12} are the only endpoints of Customer 1 that offer traffic. The total output from those CEs provides a loose upper bound on the contribution of that VPN to that PE-PE link's traffic.

Thus, for every PE-PE link PE_{kl} which is used by a VPN v, we introduce an equation that relates the traffic on that link, $N(PE_{kl})$, and the traffic between CEs that traverse the link:

$$N(PE_{kl}) = \sum_{\{(i,j) \in \Pi_{kv}\}} N(s_i, d_j) + c_{kl}$$

where Π_{kv} contains (i, j) such that $(s_i, d_j) \in v$ and s_i is routed to d_j through the PE-PE link PE_{kl}, and $c_{kl} \geq 0$ is a dummy variable. The value c_{kl} is now indicative of the contribution of all the other VPNs to the observed PE-PE traffic $N(PE_{kl})$. The traffic represented by the first term of the RHS in the above equation cannot exceed the contribution of the relevant CEs of this VPN. Thus we can substitute $N(PE_{kl})$ by $\sum_{\{(i,j) \in \Pi_{kv}\}} N^{out}(s_i)$ as a loose upper bound as discussed above (Fig. 4). Now, we have an equation with a new dummy variable $c'_{kl} \geq 0$ as:

$$\sum_{\{(i,j) \in \Pi_{kv}\}} N^{out}(s_i) = \sum_{\{(i,j) \in \Pi_{kv}\}} N(s_i, d_j) + c'_{kl} \tag{3}$$

This equation focuses on the traffic related to a particular VPN v. The summation in $N(s_i, d_j)$ signifies the traffic from s_i to

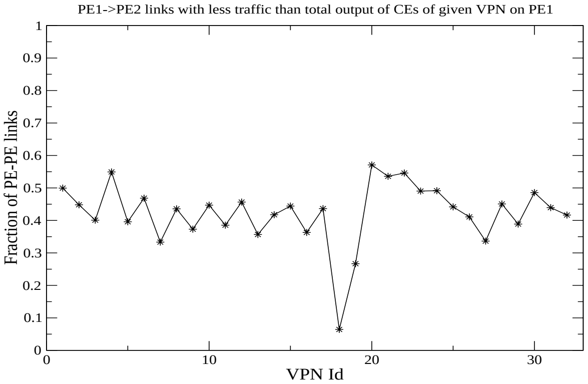


Fig. 5. Fraction of PE-PE links where traffic from CEs of a VPN on a PE is greater than the PE to PE measured traffic

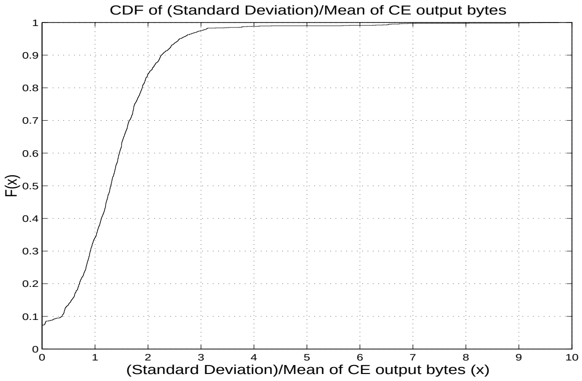


Fig. 6. CDF of the spread of spoke sizes from SNMP data for Hub/Spoke VPNs

d_j on a given PE-PE link PE_{kl}, whereas the left hand side includes all traffic generated by the CE s_i of the VPN attached to PE k.

Here, we have only used the CE-PE traffic information and not the PE-PE information. Since $\sum_{\{(i,j)\in\Pi_{kv}\}} N^{out}(s_i)$ is traffic sent towards the CEs of VPN v attached to many other PEs, it is possible that this is greater than the observed traffic on a given PE-PE link. In such cases the PE-PE observed traffic serves as a tighter constraint. Fig. 5 quantifies the significance of this constraint for large VPNs. The figure shows that in a set of (30) large VPNs we examined, there are more than 30% of PE-PE links traversed by the VPN such that the measured PE-PE traffic is less than the total output of CEs of the VPN incident on the relevant PE.

Thus we can incorporate an additional piece of information, the PE-PE traffic, to make the LHS tighter:

$$\min\{N(PE_{kl}), \sum_{\{(i,j)\in\Pi_{kv}\}} N^{out}(s_i)\} = \sum_{\{(i,j)\in\Pi_{kv}\}} N(s_i, d_j) + c''_{kl} \tag{4}$$

We are now in a position to solve the traffic matrix problem for each VPN separately. The introduction of a loose bound instead of the actual traffic due to the VPN on the PE-PE link will introduce inaccuracies in the estimated matrix. In the succeeding section we show that these inaccuracies are tolerable for purposes of a structural study of VPNs and provisioning decisions.

V. Validation of estimation technique

To verify the accuracy of the traffic matrix estimates, we could measure the actual traffic matrix and examine errors. Because we have hundreds of customers each with tens or hundreds of endpoints, the task of building a reliable measurement architecture is formidable (hence the aggregate nature of SNMP data).

One option for validating the traffic matrix estimates is to generate synthetic traffic matrices and feed it as input to a program that computes aggregate link traffic counts for the VPN. We can then evaluate the performance of the technique by comparing estimation results computed using these link traffic counts with the original synthetic traffic matrix.

A disadvantage of this approach is that real measurement data can be different from generated data. Due to the variety of possible errors in the process of collecting information, it is very hard to capture the nature of measurement noise. In §VI we supplement the synthetic validation with indirect checks on results with SNMP data to confirm that the estimation technique does indeed yield reliable estimates.

A. Synthetic Validation

We examine the performance of the estimation technique by feeding input data derived from synthetic traffic matrices. The input data involves aggregate byte counts of the links traversed by the VPN. To validate the estimation technique, we examine the error in the estimated traffic matrix compared to the actual.

We are interested in examining whether we can reliably deduce certain VPN structural and temporal characteristics despite the lack of per-VPN information for all links involved. Our strategy is as follows. Recognizing that the traffic matrix is induced by the underlying structure in the VPN, we begin by assuming a structure of the VPN and generate synthetic input data. E.g., in the following paragraphs we begin with the Hub/Spoke structure to generate synthetic inputs. If the estimated traffic between the hub and spokes agree with the actual and if the hubs are correctly identified, we conclude that the technique can be relied upon for inferences regarding Hub/Spoke VPNs.

As it will be clear in the later sections, the Hub/Spoke structure is the one that most commonly occurs among VPNs. We characterize such VPNs with the following parameters:

1) Size of the VPN
2) Number of Hubs
3) Spread in size of Spokes - the standard deviation of traffic exchanged between a spoke and a hub normalized by its mean.
4) Maximum number of CEs of a VPN homed on the same PE (“cluster size”).

We vary these parameters over a range of values that are found to be relevant to the typical VPN as seen in the measurement data. Thus we examine VPNs of size at most 15 which covers about 80% (see Fig. 3) of the sizes found in the data. We examine results for one and two hub VPNs exploiting an observation presented in a later section on classification of VPNs that 95% of the multi-hub VPNs feature 2 hubs (Fig. 7). With reference to Hub/Spoke VPNs, increased variation in the traffic volumes observed from a spoke can make it harder for the estimation technique to identify the hub.

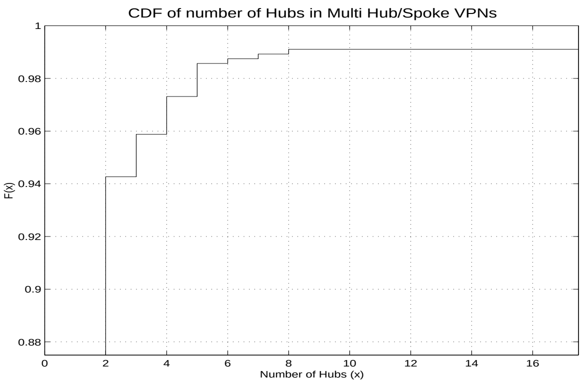


Fig. 7. CDF of number of hubs in multi-hub VPNs

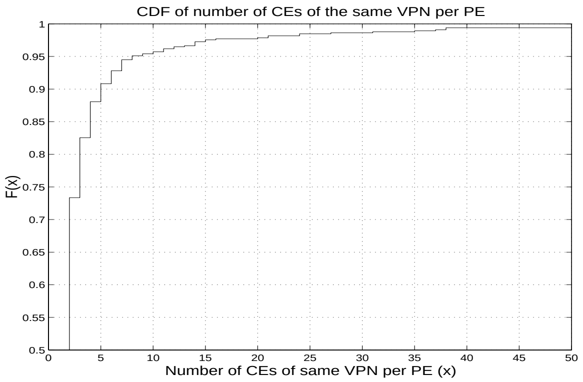


Fig. 8. CDF of number of CEs of the same VPN on a given PE

Fig. 6 shows the CDF obtained from the measured SNMP data by computing the deviation in the traffic volume across spokes for all Hub/Spoke VPNs (the methodology for classification of VPNs is discussed in the succeeding section). The deviation has been normalized by the mean. We use standard deviation to mean ratios of 1, 1.5 and 2 to examine the effect of spread of spoke sizes on accuracy. A ratio of 2 covers about 85% of the observed deviations.

The other parameter which we incorporate is the number of CEs of a VPN per PE. For a given VPN, the higher the *clustering of CEs* on a PE, the lower the number of equations at our disposal for the same number of variables. Thus it is important to see how accuracy is impacted with typical cluster sizes. Thus the number of CEs of the same VPN that are clustered on a given PE are varied from 1 to 4 to cover about 80% of the cases seen in the measurement data (Fig. 8).

1) Methodology: The generation of a synthetic sample involves generating numbers that represent aggregate bytes transmitted and received at each CE and how they are split among various other CEs of the VPN. For a Hub/Spoke VPN we first generate the data observed for the spoke nodes and then sum them up to obtain the data for the hub node.

In the results presented here, we use a mean of 1 MB for the aggregate bytes transmitted and received at each CE that is a spoke. We set the standard deviation for spoke traffic using the CDF obtained from the SNMP data. The specific value of the mean has no impact on the results. To summarize the procedure:

1) Set mean μ and standard deviation σ for spoke traffic
2) Generate a Gaussian random number $r_i \sim (\mu, \sigma)$ for each spoke i, where r_i represents the spoke traffic.
3) $R \leftarrow \sum_i r_i$
4) R gives the traffic attributed to the hub

In order to implement the maximum cluster size, we use a uniform random variable as follows. Given a maximum number of CEs m that can be assigned to the PE, we generate an integer random number in $(1, m)$ for each PE. The CEs are assigned to the PEs sequentially till all CEs have been assigned. We summarize the procedure below:

1) Set max number of CEs of a VPN per PE as m, size of VPN as sz
2) Set $i \leftarrow 1$ (CE index), $j \leftarrow 1$ (PE index)
3) Generate an integer random number $r \sim Uniform(1, m)$
4) Set $r \leftarrow min(i + r - 1, sz)$
5) Assign $CE_i, CE_{i+1} \ldots CE_r$ to PE_j, set $i \leftarrow r + 1$
6) If $i < sz$, set $j \leftarrow j + 1$ and go to 3

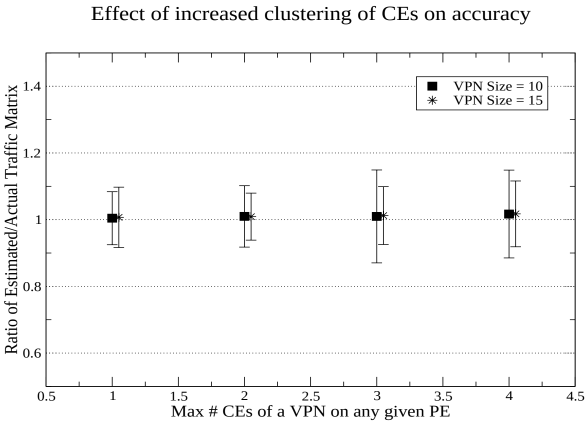


Fig. 9. Error in estimated traffic matrix increases with increased clustering of a customer's endpoints on a PE

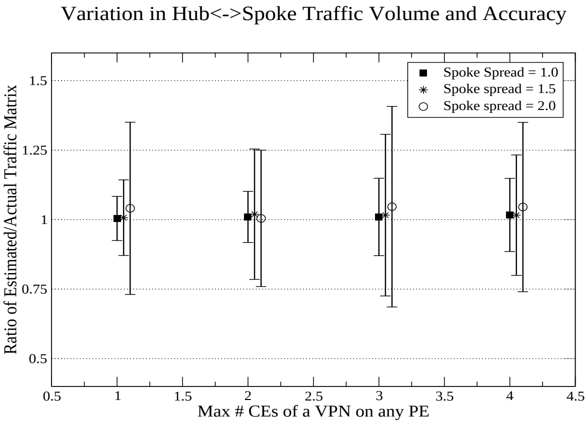


Fig. 10. Effect of cluster size with varying spread in spoke sizes for VPN of size 10. Smaller VPNs are affected more by increase in spread in spoke size

2) Single Hub VPNs: We begin our evaluation on estimation error by examining the effect of the number of CEs of a given VPN incident on the same PE (clustering). Recall that each link traversed by the VPN gives us one equation

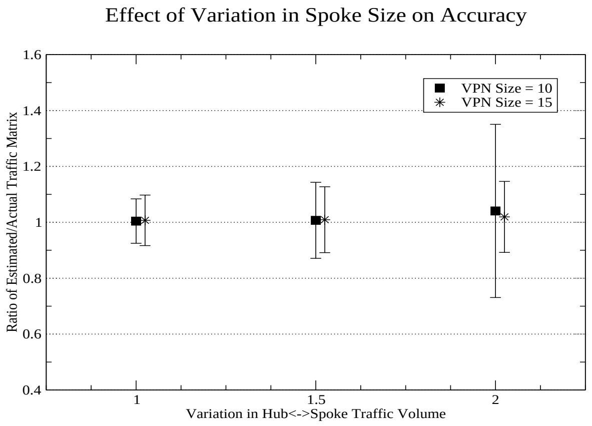


Fig. 11. Size of the VPNs and clustering of CEs are more influential w.r.t the accuracy of the TM estimates.

relating the traffic matrix variables. Higher clustering thus gives us fewer equations for the same number of variables causing higher errors in estimation. Further, a given cluster size has greater impact on estimates if the size of the VPN is smaller. We employ the ratio of the estimated traffic matrix to the actual as a measure of the error - the closer the value to one, the better the estimate. Fixing the spread of spoke sizes at 1, Fig. 9 indicates that while the standard deviation of the error increases for higher clustering, it is around 10% even at higher cluster sizes for the larger VPN. From the perspective of PE-PE bandwidth provisioning, even the errors at higher cluster sizes are often tolerable. Even if higher accuracy is desired for provisioning, other tasks (maintenance, re-homing etc.) can take full advantage of the traffic matrices that we derive here.

On the other hand, varying the spread (standard deviation) of spoke sizes for the smaller VPN, shows that accuracy suffers with increasing spread (Fig. 10). This is due to the fact that in a smaller VPN, increased variation in spoke sizes can translate to some of the spokes being comparable to the hub. Larger VPNs are less susceptible to such variations in spoke sizes. Fig. 11 confirms this observation by depicting the effect of variation in spoke sizes with increase in VPN size.

Thus the synthetic validation points to the following observations: (a) the estimates are reliable for Hub/Spoke VPNs over a significant range of parameter values covering a majority of such VPNs; (b) with smaller VPN size, the spread of spoke sizes and cluster size can impact the accuracy of the estimates; (c) estimates for larger Hub/Spoke VPNs are resilient to variations in cluster size and spread in spoke sizes, and hence are better.

We elaborate on hub identification in §V-A.6 and §VII.

3) Two-hub VPNs with dual-homed hubs: In general the evaluation with synthetic data indicates that, with consistent input, the accuracy of estimating the traffic matrix is very good in the case of Hub/Spoke VPNs. These conclusions also apply in a limited sense to multi-hub VPNs where the multiple hubs act as one unit with a load-balancing entity presenting a single interface to the spoke nodes. In such cases, if the hubs are considered as one unit and traffic matrix variables defined accordingly, these conclusions apply fully.

% VPNs with multiple hubs	$\approx$ 18%
% Multi-hub VPNs with 2 hubs	$\approx$ 95%
% of 2 hub VPNs dual homed	$\approx$ 40%
% of all VPNs analyzable	$\approx$ 57%

TABLE II
MULTI-HUB VPNS AND DUAL HOMED HUBS

An analysis of the measured SNMP data shows that a majority of the Multi-hub/Spoke VPNs feature only two hubs (Fig. 7). Further, among these two hub VPNs, 40% have both the hubs homed on the same PE indicating that they are in the same facility. Such dual homed hubs act as one unit with spoke traffic being load balanced among them. In essence, the analysis in the previous section indicates that traffic matrix estimates will be accurate for these VPNs. Utilizing the results of classification of VPNs (to be discussed in §VII) we see that about 57% of all VPNs can be accurately handled with our proposed estimation techniques (Table II).

4) Multi-hub VPNs without dual-homed hubs: The remaining type of Multi-hub VPNs are those that have two or more hubs where the hubs communicate with different subsets of CEs in the VPN. Unlike two-hub VPNs with dual-homed hubs, the hubs in these VPNs do not appear as a single entity to the spokes. These hubs are possibly geographically spread out and feature distinct sets of spokes communicating with them.

We found that the estimation technique cannot provide reliable results in such VPNs. A typical example would be where a subset of CEs transmits zero bytes to one hub and all bytes to a second hub. Due to the absence of per-VPN information on the PE-PE links, the estimation technique has no way of discovering whether a given CE has indeed transmitted to another CE. The traffic matrix estimate for a given CE pair is driven in part by their traffic volume and the equations for aggregate link counts. Hence, the estimation procedure gives a non-zero estimate so long as the traffic volumes from the CEs are non-zero. In the Hub/Spoke case, this does not drastically affect the errors since the size of the hub is very large relative to spokes.

5) Validation for Large VPNs: We have examined results for hub/spoke VPNs, which are the typical cases reflected in the measurement data. There are some aspects of the traffic that aid in solving for large VPNs. We find that not all CEs communicate in a given measurement interval. The result is that the number of variables to be solved for reduces to a large extent (since they are known to be zero).

Fig. 12 shows the CDF of fraction of CEs that featured non-zero output bytes in the SNMP data for small, medium and large VPNs (lower, middle and higher 33%-ile). The figure shows that in small and medium sized VPNs, 70% or more of the CEs feature non-zero traffic with probability 0.8. For the large VPNs, we see 70% or more of the CEs transmitting some data with probability 0.65. This means that with larger VPNs, there are more CEs that transmit no data in a given interval, leading to simplification of the system to be solved.

Coupling this with observations in §V-A.2 which showed that estimates for larger Hub/Spoke VPNs are resilient to spread in spokes and a range of cluster sizes, we see that traffic matrices can be expected to be more accurate in larger Hub/Spoke VPNs. We have not performed the synthetic

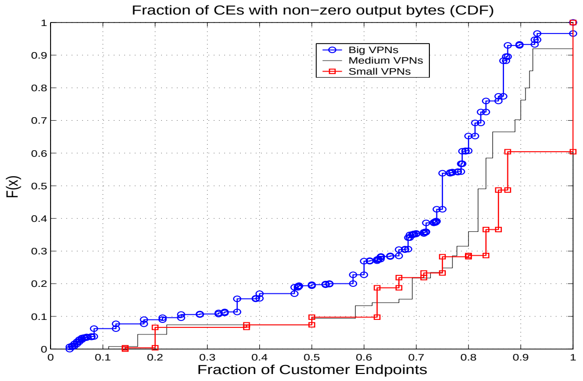


Fig. 12. CDF of fraction of CEs featuring non-zero output bytes confirms bigger hub/spoke VPNs have more CEs with zero output bytes. This means that accuracy of estimates for bigger Hub/Spoke VPNs is better.

VPN type	% VPNs where node with max peers had:	
	Max CIR	Max PIR
Pure Hub/Spoke	72.2	66.1
Dual Hub/Spoke	77.4	77.4
Hybrid	49.5	42.3

TABLE III
RELATION BETWEEN CIR AND NUMBER OF PEERS

validation for larger VPN sizes here (which are the top 20% in the measurement data) since it is hard to generate a realistic data-set.

6) Significance of observations:

1) *Clustering of CEs of same VPN:* While provisioning a VPN, the provider usually attempts to reduce clustering of CEs onto a PE so as to reduce the risk of outage for the customer. This bodes well for measurement techniques that have to work with limited information as indicated by the results in the previous sections.
2) *Identifying a hub:* Since the size of the hub is very large compared to the spokes in a Hub/Spoke VPN, a thresholding criterion can be reliably used to identify the hub. Given the traffic matrix estimates for a CE toward all other CEs, we can form a set of its peers by pruning all CEs toward which estimates are comparable to errors in estimating the traffic matrix. The node with almost all CEs as peers would be the hub. Such a thresholding technique is preferable over an alternative that considers the Committed or Peak Information Rates (CIR/PIR), or just the total traffic volume for the CE. This is supported by the following measurement-based observations:
   - An examination of CEs and the CIR or PIR value (Table III) indicates that a significant fraction of the nodes with the maximum CIR or PIR are not nodes with the most peers (approximately 28% in the case of pure Hub/Spoke VPNs do not have the maximum CIR or PIR).
   - Traffic volume entering or leaving the nodes that are hubs is not symmetric. Hence it is not possible to rely on either or both these measures to judge whether a CE is a hub. This is indicated in Fig. 13 which shows that roughly 80% of the Hub/Spoke VPNs feature hubs where the number of bytes entering the hub differs from the number of bytes leaving the hub by more than 10%.
3) *Multi-hub and other VPNs:* Clearly more data is needed to reliably analyze multi-hub VPNs and other complex structures. With the current data, one could obtain the traffic matrix and use it only to obtain an approximate set of hubs.

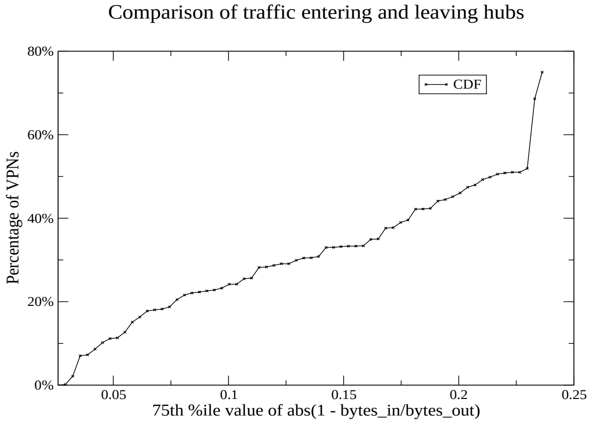


Fig. 13. CDF of 75^{th}%ile ratio of traffic entering a hub to the traffic leaving a hub for Hub/Spoke VPNs

VI. COMPARING ESTIMATES WITH SNMP DATA

We now examine SNMP data to complement the synthetic validation in the previous section. We obtain traffic matrix estimates and aggregate them on a per-link basis to compare against SNMP measurements. We begin with a set of sanity checks on the data set.

A. Cleaning the dataset

Given the large-scale nature of the data that is being handled, it is natural to expect errors and inconsistencies in the collection process. It is very important to remove samples that are a manifestation of such errors so that we can understand the performance of our algorithms clearly. In order to clean the dataset, we take recourse to certain properties a valid dataset must satisfy:

1) Noting that CEs in a VPN receive traffic only from other CEs in the same VPN, we observe that whatever data any CE receives must come from a member of the VPN. Thus, the total bytes received by the CEs should be less than or equal to the total bytes transmitted by the CEs, in the same VPN.
2) For any given PE, the total bytes transmitted into the network should be less than or equal to the total bytes offered by all the CEs (of various VPNs) attached to the PE. This is considering the fact that a PE does not generate data.
3) For any given PE, the total bytes transmitted toward CEs attached to it should be less than or equal to the bytes it received from the network.

In reality a fraction of our dataset does not strictly conform to all these rules. We had to relax the rules so that we have a good number of samples to work with, while still being

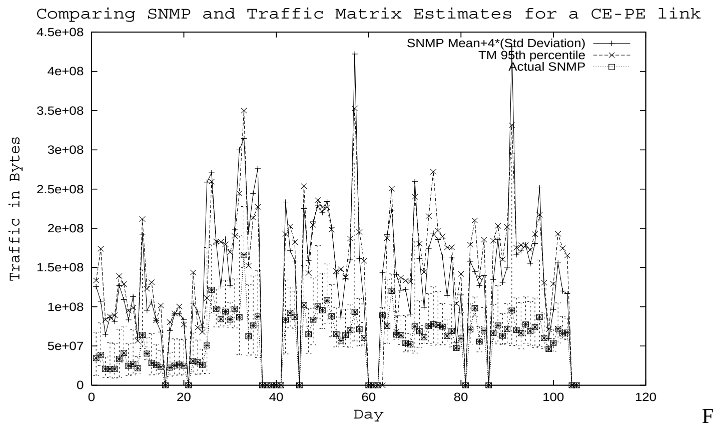


Fig. 14. Comparison of estimated CE output bytes with that derived from SNMP

confident that the samples are meaningful. The strategy we use is to allow a range of error - we consider 10% error to be tolerable here.

Additionally, each VPN is a geographically spread out entity. This means that measurements are usually not time synchronized and are sometimes absent due to problems with polling and dropped packets. Some error cases are handled by the measurement modules and are indicated in the data. Such samples are discarded and the rest of the samples are subject to the above tests. Depending on the objectives of the analytical exercise, the threshold for error tolerance can be set to a different value.

B. Validation with SNMP data

In §V we could test the accuracy of traffic matrix estimates by comparing them with the actual synthetic traffic matrix that was used to generate the test input. The SNMP measurement data on the other hand does not provide per-VPN information, i.e., we do not know the actual traffic matrix for the VPNs being analyzed. From the results of §V we know that estimates are reliable for a large fraction of Hub/Spoke VPNs. We first examine indirect means of confirming this conclusion. This involves looking at the SNMP measurement of CE-PE link traffic and comparing it with the estimates. We then compare the observed PE-PE link counts with traffic matrix estimates, keeping bandwidth provisioning in mind.

1) CE-PE link data: Fig. 14 examines the CE-PE aggregate traffic. The traffic matrix estimate provides us with values for all variables $N(s_i, d_j)$. Thus for a given s_i if we sum the variables $N(s_i, d_j)$ for all d_j, it should give the CE-PE link count for s_i. We compute traffic matrices for each hour of the day across 105 days and plot the sum of the 95^{th} percentile values of the relevant $N(s_i, d_j)$ values for a small and large VPN. The plots show that the mean plus four times the standard deviation of the observed SNMP measurements agrees closely with the 95^{th} percentile values obtained from the estimates. This means that the results of estimation are accurate in the aggregate, as we would expect given the way the optimization formulation was built.

2) PE-PE link traffic: We now compare the traffic on PE-PE links based on the estimated matrices to measured SNMP data for the traffic on these links. As noted previously, the CE to CE path consists of a core network segment where it is shared among multiple VPNs. By summing all $N(s_i, d_j)$ variables of a VPN that traverse a given PE-PE link, we obtain the estimated contribution of a VPN to a given PE-PE link. We then consider all VPNs that share this link and repeat the same procedure. Summing across all such results across VPNs, we obtain the estimated PE-PE traffic and examine it with reference to SNMP data. Fig. 15 depicts a PE-PE link with lower traffic volumes and Fig. 16 for higher traffic volumes. The accuracy of PE-PE traffic estimates reduces for links with less traffic. The errors are markedly less for links with higher traffic as depicted in Fig. 16. This is due to the fact that the errors in SNMP measurement become comparable to traffic volume of smaller links. However, both graphs show that the estimated numbers follow the same pattern of variation as the measured numbers in time over a complete day.

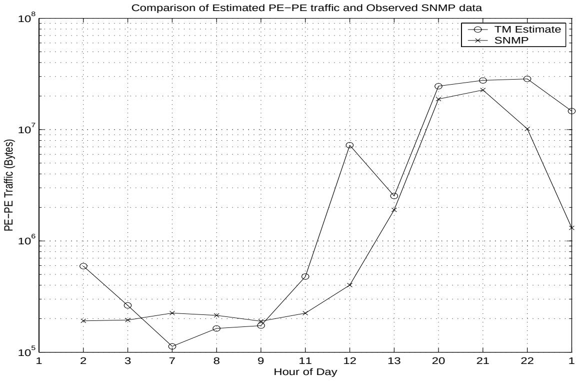


Fig. 15. Estimated traffic vs Observed traffic for a PE-PE link with lower traffic volume

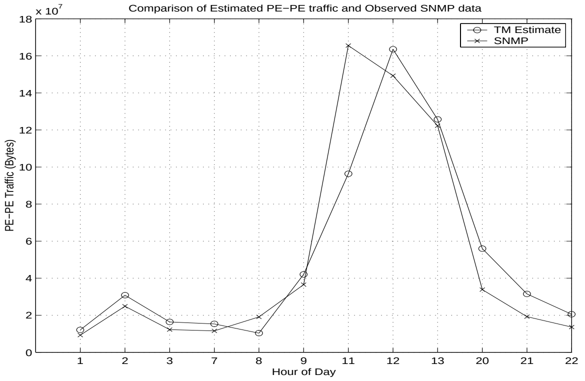


Fig. 16. Estimated traffic vs Observed traffic for a PE-PE link with higher traffic volume features better accuracy; estimates mimic the shape and order of the actual traffic in all cases

Reasonable accuracy in estimating the aggregate PE-PE links has implications for bandwidth provisioning tasks. Typically, core capacity provisioning involves a factor of safety, and estimates to drive such a task need not be exact. A factor of 2 error in the estimate is usually considered tolerable. With this goal in mind, we repeat the PE-PE validation procedure with approximately 700 links and obtain Fig. 17. This figure indicates the ratio of the TM estimate to the observed PE-PE SNMP traffic for various link volumes. We note the following from this graph:

- For a large number of links, the estimated PE-PE traffic

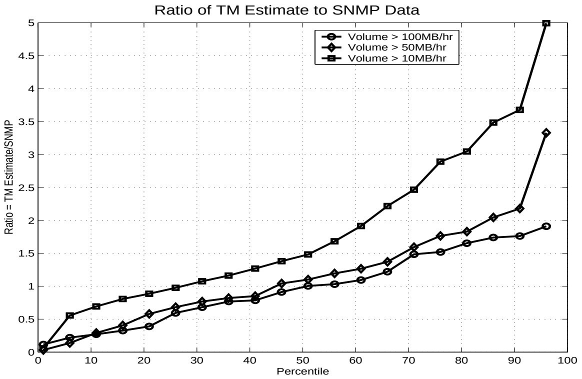


Fig. 17. The error decreases when we look at links with larger volume

is within 50% of the SNMP observed traffic and most of the cases it is either close to the SNMP quantity or greater.

- Significant under-estimation happens for around 25% of the links considered and these cases were traced to three problems in the data for VPNs traversing those links: (a) the PE-CE and CE-PE SNMP data was zero even when the PE-PE data seemed to be significant; (b) there were more bytes transmitted from the PEs to the CEs than what was received by the PE (measurement inconsistency); (c) the total bytes received by CEs was greater than the total bytes transmitted, i.e., there were external sources not accounted for in the SNMP data.
- Significant over-estimation occurs when the traffic volume on the link being considered is “small”. By “small” we mean it is comparable to errors in SNMP data. E.g., in cases where the difference in the number of bytes input to a PE and the number of bytes leaving it is 10MB and the PE-PE traffic volume was also about 10MB.

The validation considered here is not complete since we do not have actual per-VPN traffic data. Due to the scale of the exercise it is unlikely that such data will be available in the near future. In addition, owing to the mission critical and private nature of VPN traffic, there are a lot of administrative hurdles to obtaining access to such traffic. Thus, we need to examine traffic matrix estimates in the current framework and evolve guidelines to gauge the reliability of the estimates.

C. *Reliability of Traffic Matrix Estimates*

Estimation techniques such as those described in this paper deal with aggregate byte counts and some additional side information to arrive at the components that led to that aggregate byte count. Even if the SNMP counts match the estimates, it is not necessary that the individual VPN matrices be correct. But we employed multiple strategies to gain confidence in our technique, viz., validation with synthetically generated data and indirect measures involving CE-PE and PE-PE SNMP data.

Observe that so long as most of the VPNs being analyzed exchange the bulk of their traffic on PE-PE links, the estimates are reliable if per-customer clustering of CEs is low. This is because, the traffic passes three segments: (a) the CE-PE link, (b) the PE-PE link and (c) the PE-CE link on the destination side. Now (a) and (c) are part of the constraints in the optimization formulation. So any solution that has the property that the variables sum to the observed access link aggregate may be acceptable. Now, consider the case when the PE-PE link counts match reasonably. If there are a number of CEs *of a given VPN* attached to a PE, we might still have errors in estimation - we could assign more bytes to a particular CE and still satisfy all constraints of the optimization. But if the number of CEs on a PE is small, then since all the segments of the transit route match with measurement, we must have a good estimate. Thus we evolve a set of guidelines to gauge the reliability of the estimates exploiting the observations of the previous sections.

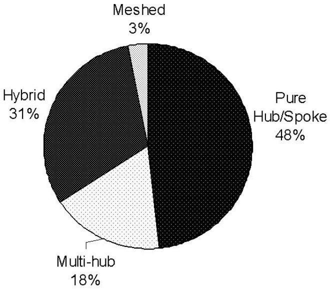


Fig. 18. Structural classification of all VPNs

1) If the number of CEs of a Hub/Spoke VPN homed on the same PE is low, the traffic matrix estimates are reliable.
2) Given consistent measurement data, PE-PE aggregate traffic can be estimated with reasonable accuracy for provisioning purposes.

In the current dataset, we have found the number of CEs of a given VPN per PE to be low and that a significant percentage of VPNs are of a hub/spoke nature. Hence we are in a position to study the structural characteristics and temporal characteristics of these VPNs.

VII. Spatial Structure for Classification

Based on the way VPN endpoints communicate with each other (using the derived traffic matrices), three broad categories for the VPN structure can be deduced: (a) Pure Hub/Spoke, (b) Multi-Hub/Spoke, and (c) Hybrid VPNs. As the name suggests, a pure Hub/Spoke VPN features “spoke” nodes that communicate with just one node called the “hub”. With Multi-hub/Spoke VPNs, there are two or more hubs with which all the CEs communicate. VPNs that cannot be grouped into either of these categories are termed Hybrid VPNs.

To identify the structure of a VPN, we obtain the set of peers for each CE by examining the estimated traffic toward all other CEs in the VPN. Note that the estimation procedure provides non-zero estimates so long as the input and output bytes of a given CE pair are non-zero. Hence even though a pair of CEs do not communicate with each other in reality, the estimate might attribute a non-zero value to the pair. Fortunately, the fact that hub traffic is far greater than that of spokes causes these spurious estimates to be small in the case of Hub/Spoke VPNs. Hence we build an approximate set of peers for a CE after pruning lower values which are more likely to be estimation errors.

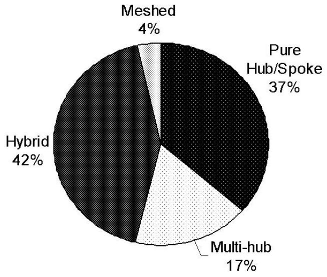


Fig. 19. Structural classification of big VPNs

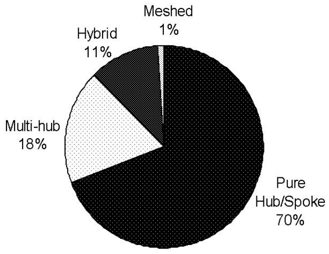


Fig. 20. Structural classification of small VPNs

Thus, given traffic matrix estimates for a VPN, we employ the following procedure to identify its structure. We obtain the set of peer CEs for every CE after eliminating zero values and pruning the bottom 25% in terms of estimated traffic volume and classify a CE as follows:

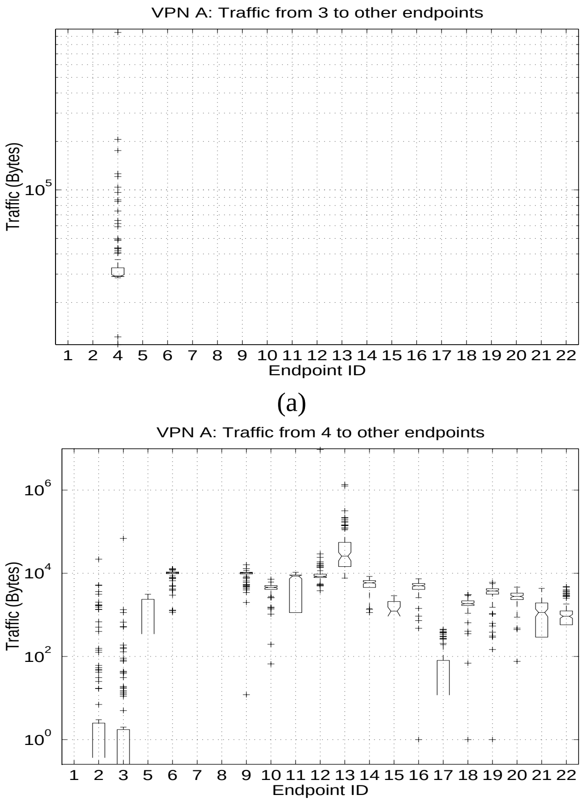
1) If a CE communicates with more than 50% of the endpoints in the VPN, it is judged to be a hub node.
2) If a CE has 1 or 2 peers, it is classified as a spoke.
3) If a CE is in neither of the above categories it is classified as hybrid.

We then classify the overall VPN as follows:

1) If a VPN has a hybrid CE, it is a hybrid VPN
2) If a VPN has exactly one hub and all other CEs are spokes, it is a pure hub/spoke VPN.
3) If it has more than one hub but the number of hubs is less than 50% of the size of the VPN, we judge the VPN to be of the Multi Hub/Spoke nature.
4) If more than 50% of the nodes in the VPN are "hubs", we say the VPN is of the meshed kind.

Fig. 18 shows the result of this analysis of around 600 VPNs in the dataset. The classification indicates that a significant number of the VPNs are of the Hub/Spoke nature. Frequently, the VPNs have 2 or 3 hubs for redundancy and load balancing.

The classification indicates that with larger VPNs (upper 33%-ile by number of CEs- Fig. 19), the structure becomes very complex and there are more of these classified as hybrid. Across various sizes of VPNs, there is a significant fraction that is of the hub/spoke nature (either Pure or Multi Hub/Spoke). This has implications for provisioning and traffic engineering as we shall note in §VIII-A. Small VPNs (lower 33%-ile - Fig. 20) tend to exhibit simple structures. As examples, we look at the communication structure of a few small VPNs. VPN A shown in Fig. 21(a) exhibits a hub/spoke structure. Fig. 21(a) features traffic flowing from a "spoke" to endpoint 4, which we characterize as a hub. The hub node on the other hand communicates with most other endpoints as shown by Fig. 21(b). The plots have been generated using traffic matrix estimates over many days. Hence there are notched boxes that denote the range of values for traffic observed toward a given endpoint. The notched box usually features three horizontal lines indicating the 25, 50 and 75 percentile values. Fig. 22 shows the traffic from three endpoints in a VPN of size 4 illustrating a mesh type of communication among the endpoints. Each plot depicts the traffic from a given endpoint to other members of the VPN. Often VPNs cannot be categorized in either of these categories. VPN C featured in Fig. 23 shows a given endpoint communicating with many other endpoints with orders of magnitude difference in the traffic volumes.



(a)

(b)

Fig. 21. Hub/Spoke-like behavior can be seen with some endpoints in VPNs such as above

Such structural characteristics are very important to efficiently provision network resources. Instead of a mesh of N^2 reservations for a N node VPN, we could tailor allocations depending on the structure of the VPN resulting in a simplification in provisioning [6].

VIII. Temporal Structure and Provisioning

For a new VPN there is not much information regarding traffic characteristics and hence provisioning has to be approximate and conservative. In order to ensure SLAs, the provider needs to learn customer demands and how they change over time. In the case of new VPN customers, the initial conservative resource allocation can be fine-tuned over time by learning

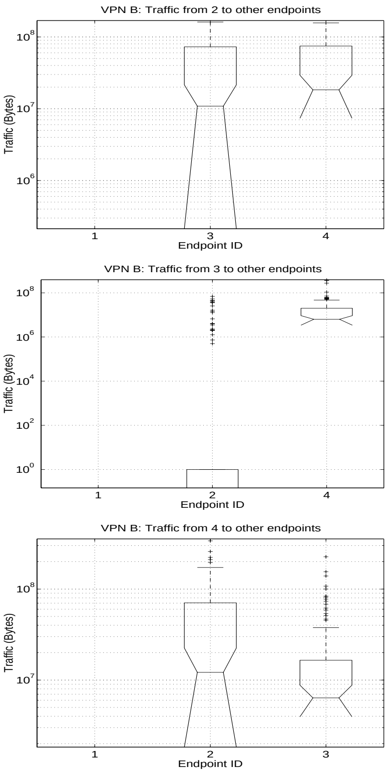


Fig. 22. Small VPNs have simple structure. The one depicted above has 3 of the 4 nodes in the VPN forming a mesh

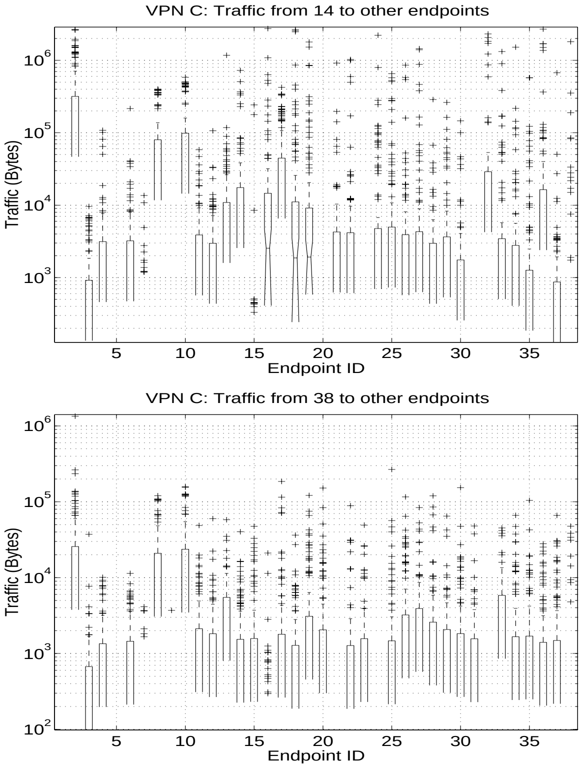


Fig. 23. A larger VPN exhibiting complex interactions between various endpoints. There are orders of magnitude difference in the amount of traffic toward different CEs

customer characteristics so that the provisioning better reflects actual demands. Faster changes in traffic characteristics imply that provisioning needs to be more responsive. Links may need to be resized to accommodate existing customers. On the other hand, slower changes in traffic would allow the provider to exploit multiplexing gains and increase the number of customers served. Thus we are interested in studying the changes in traffic matrices over time to judge whether complex dynamic provisioning strategies can yield appreciable gains.

Fig. 24 demonstrates the traffic matrix for an endpoint in a Hub/Spoke VPN for various times of the day. In this figure, SNMP data collected between 6am and 10am are counted for morning traffic, the data from 11am and 2pm is considered as mid-day and the duration between 8pm-12 midnight is considered as night. Each point in these graphs is the median of the number of bytes seen in those hours, computed using a set of weekdays. The error bars (the vertical lines) indicate the 25^{th} and the 75^{th} percentile values. When the 25^{th} percentile value is too low compared to the median, the error bar is truncated and this is indicated by a downward arrow. Fig. 24 indicates that the relative ratios across the endpoints does not change substantially over the period of the day.

The trends (the proportion of traffic to a given endpoint relative to the others) show a similar shape although there are differences in magnitude indicating that time of day is a distinguishing factor. With this observation, we now consider traffic matrix changes over longer timescales. In Fig. 25 we examine traffic trends across multiple weeks for a given endpoint. Each curve shows the median traffic toward an endpoint with the error bars indicating the percentiles as above. Barring one point, the trend for morning traffic across weeks is strikingly similar. This means that the trends change slowly, so that intelligent provisioning schemes have enough time to learn the traffic characteristics and act accordingly.

Extending the analysis over several months gives us some more insight. Fig. 26(a) and Fig. 26(b) depict trends for traffic from a given endpoint in two VPNs of different sizes toward the rest of the endpoints. While trends in one of the VPNs are stable over time in both shape and magnitude, the second plot shows magnitude variations over weeks with the later weeks featuring higher traffic. In such cases where either VPN traffic grows over time or VPNs add new endpoints over time, learning traffic matrices is very useful. Additionally this also means that even if initial provisioning is conservative, growth in VPN traffic might render it insufficient if adaptive mechanisms are not in place.

A. Impact on Provisioning

The discussion in the previous paragraphs leads us to the following important observations:

- **Traffic Engineering:** The traffic matrices provide us an estimate of the size of the customer aggregate in the core network. This allows us to conduct traffic engineering on a per-customer aggregate basis: we can re-map traffic for a given customer on to a new logical path and have an estimate of the added load and available capacity. Without this information, traffic engineering would have to handle PE-PE aggregates as a whole.
- **Bandwidth Allocation:** Exploiting spatial characteristics can lead to simplified provisioning and efficient resource allocation, especially in the case of endpoints which

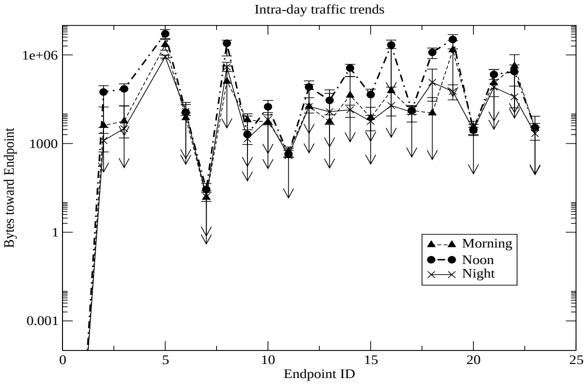


Fig. 24. An Endpoint communicating with multiple peers; traffic proportions to other endpoints are very similar for different times of day, although the magnitude varies.

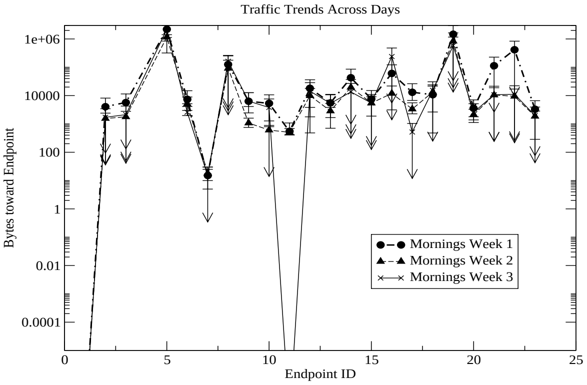


Fig. 25. Traffic trend from an endpoint to others in a VPN remains similar across multiple days.

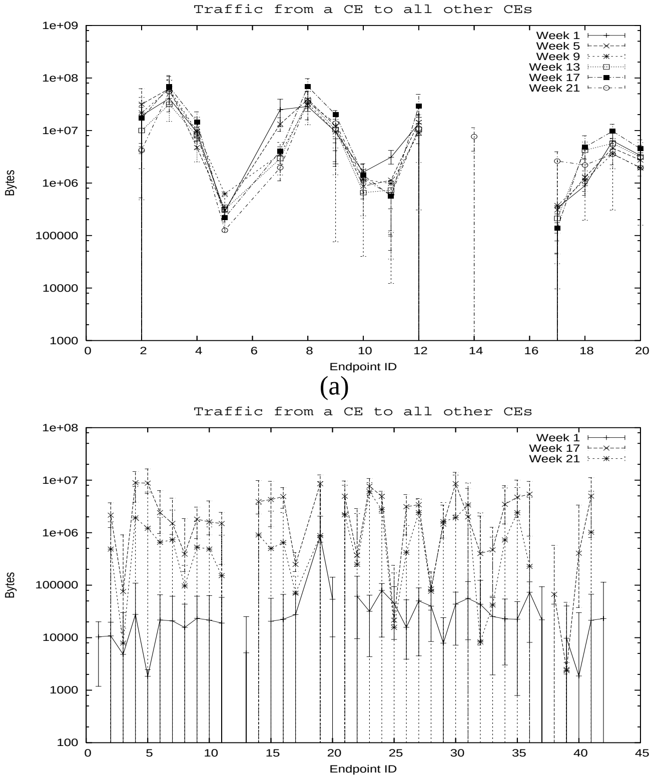
communicate with just one or two other peers. Addition of new endpoints in the VPN and growth in customer demand over time are better handled by learning traffic characteristics.

- **Customer Differentiation:** Since the traffic matrices provide an estimate of the size of the customer aggregate in the core network, the provider can choose to provide preferential treatment to a selected set of customers more efficiently. For the chosen set of customers, the provider keeps track of the aggregate demands using traffic matrices and makes allocations appropriately. The temporal characteristics of the traffic matrix indicate that the aggregate characteristics vary slowly and can be learnt.
- **Managing network failures:** The additional knowledge of customer traffic can lead to elegant management of network failure and maintenance events. E.g., the aggregates leading to a hub node can be mapped on to a new path which has more available capacity.

IX. Summary and Conclusions

This paper analyzed two important properties of VPNs: (a) the structure of customer endpoint (CE) interactions and (b) the temporal characteristics of CE-CE traffic. Understanding actual customer behavior for large scale VPNs can help in many ways including dealing with traffic engineering, bandwidth allocation, moving a service to a different infrastructure, and other provisioning and maintenance operations.

We began with SNMP measurement information for 5 months from a large IP VPN service provider featuring about 6000 logical links. The VPNs had customer end points ranging from a few tens to several hundred CEs. With such a realistic, large scale service, there are significant barriers to obtaining detailed, per-customer measurement information. Consequently, there is only coarse grained aggregate SNMP data of traffic on the internal PE-PE links of the service. To get structural and temporal information about individual VPNs, we needed to evolve previous traffic matrix estimation approaches to overcome the problems posed by the scale of our problem (the matrix for the entire problem is in the range of nearly 3 Million elements.) Based on the characteristics of VPN traffic, we developed bounds on the traffic generated by a VPN on an individual PE-PE link, and used these in our technique to estimate the traffic matrices.



(a)

(b)

Fig. 26. Long term trends for traffic from a CE to all other CEs in VPNs of higher size

Without actual per-VPN measurements, it was difficult to directly validate our traffic matrix estimation approach. We adopted a two-pronged approach. First, we used a synthetic data set to compare the traffic matrices obtained by our technique to the actual, a-priori known traffic matrix. The synthetic data set we used was based on the broad characterization obtained from the SNMP measurement data, to allow us to have greater confidence in our approach. We showed that our approach works very well for Hub/Spoke VPNs. Second, we examined indirect measures by deriving aggregate CE-PE and PE-PE traffic volumes from the estimated traffic matrices, and then compared it with the measured aggregate SNMP count. Our estimates for the mean and the 95^{th} percentile of the CE-PE traffic agreed closely with the actual values. We also showed that estimates for the aggregate PE-PE traffic were reasonably accurate. They were more accurate for links of higher capacity, and are able to reflect the temporal characteristics that are actually present in the traffic.

We then analyzed spatial and temporal characteristics of customer VPNs. We identified three broad categories of VPNs: pure hub/spoke, multi-hub/spoke and hybrid VPNs. Overall, approximately 48% of the VPNs are of the pure hub/spoke category. But for small VPNs (the bottom 33% of the VPNs based on size), hub/spoke VPNs dominate (70%). Of the multi-hub VPNs (18% of all VPNs), interestingly 95% are 2-hub VPNs. A significant portion of the big VPNs (top 33% of VPNs) are Hybrid VPNs (that are neither hub/spoke nor meshed VPNs). The percentage of pure "meshed" communication where any node talks to any other node is relatively small (at 3%).

An examination of the temporal properties of traffic matrices showed that they are quite stable over the period of a day, and even across days over a period of weeks. Thus, we can use this measurement data to get an idea of the "stable" VPN structure for each customer VPN, and thus, have a reasonable estimate of the demand of each VPN customer endpoint on access and core links. We believe that this paper is unique in providing an understanding of VPN characteristics from an operational, large scale VPN service.

X. Acknowledgments

We wish to express sincere thanks to Dr. Chris Chase of AT&T Labs Research for making available to us all the measurement information employed in this study and for extremely useful operational insights that provided direction to our investigations.

References

[1] S. Raghunath, K. Ramakrishnan, S. Kalyanaraman, and C. Chase, "Measurement based characterization and provisioning of IP VPNs," in *Proc. of IMC 2004*, 2004, pp. 342–355.

[2] E. Rosen and Y. Rekhter, "BGP/MPLS VPNs," RFC 2547, Mar. 1999.

[3] N. Duffield, P. Goyal, A. Greenberg, P. Mishra, K. Ramakrishnan, and J. van der Merive, "Resource management with hoses: point-to-cloud services for virtual private networks," *IEEE/ACM Trans. Networking*, vol. 10, no. 5, pp. 679–692, Oct. 2002.

[4] S. Raghunath, K. Chandrayana, and S. Kalyanaraman, "Edge-based qos provisioning for point-to-set assured services," in *Proc. of ICC 2002*, vol. 2, Apr. 2002, pp. 1128–1134.

[5] S. Raghunath and S. Kalyanaraman, "Statistical Point-to-Set edge-based quality of service provisioning," in *Proc. of QoFIS 2003, Springer Verlag LNCS 2811*, vol. 2, Oct. 2003, pp. 132–141.

[6] S. Raghunath, S. Kalyanaraman, and K. Ramakrishnan, "Trade-offs in resource management for virtual private networks," in *Proc. IEEE INFOCOM 2005*, 2005.

[7] Y. Zhang, M. Roughan, C. Lund, and D. Donoho, "An information-theoretic approach to traffic matrix estimation," in *Proc. of ACM SIGCOMM 2003*, 2003, pp. 301–312.

[8] A. Medina, N. Taft, K. Salamatian, S. Bhattacharyya, and C. Diot, "Traffic matrix estimation: Existing techniques and new directions," in *Proc. of ACM SIGCOMM 2002*, Pittsburgh, USA, Aug. 2002.

[9] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, and F. True, "Deriving traffic demands for operational IP networks: methodology and experience," *IEEE/ACM Trans. Networking*, vol. 9, no. 3, pp. 265–279, June 2001.

[10] Y. Vardi, "Network tomography: estimating source-destination traffic intensities from link data," *J. Amer. Statist. Assoc*, vol. 91, pp. 365–377, 1996.

[11] C. Tebaldi and M. West, "Bayesian inference on network traffic using link count data," *J. Amer. Statist. Assoc*, vol. 93, no. 442, pp. 557–576, 1998.

[12] J.Cao, D.Davis, S. Wiel, and B.Yu, "Time-varying network tomography," *J. Amer. Statist. Assoc*, vol. 95, no. 452, pp. 1063–1075, 2000.

[13] M. Bertero, T. Poggio, and V. Torre, "Ill-posed problems in early vision," vol. 76, no. 8, pp. 869–889, Aug. 1988.

[14] I. Craig and J. Brown, *Inverse Problems in Astronomy: A Guide to Inversion Strategies for Remotely Sensed Data*. Boston: Adam Hilger, 1986.

[15] A. Neumaier, "Solving ill-conditioned and singular linear systems: A tutorial on regularization," *SIAM Review*, vol. 40, no. 3, 1998.

[16] Y. Zhang, M. Roughan, N. Duffield, and A. Greenberg, "Fast accurate computation of large-scale IP traffic matrices from link loads," in *Proc. of ACM SIGMETRICS 2003*, 2003, pp. 206–217.

[17] A. Kumar, R. Rastogi, A. Silberschatz, and B. Yener, "Algorithms for provisioning virtual private networks in the hose model," in *Proc. of ACM SIGCOMM 2001*, 2001, pp. 135–146.

[18] A. Gupta, J. M. Kleinberg, A. Kumar, R. Rastogi, and B. Yener, "Provisioning a virtual private network: a network design problem for multicommodity flow," in *ACM Symposium on Theory of Computing*, 2001, pp. 389–398.

[19] L. Zhang, J. Muppala, and S. Chanson, "Provisioning virtual private networks in the hose model with delay requirements," in *Proc. of ICPP 2005*, 2005, pp. 211–218.

[20] T. Erlebach and M. Ruegg, "Optimal bandwidth in hose-model VPNs with multi-path routing," in *Proc. IEEE INFOCOM 2004*, vol. 4, 2004, pp. 2275–2282.

Satish Raghunath is a Member of Technical Staff at Juniper Networks. He holds a PhD degree from Rensselaer Polytechnic Institute (Troy, NY) and a B.E. in computer engineering from NITK Surathkal. He worked on dynamic provisioning issues and cross-layer network resource management at Nortel. His current interests include network security, quality of service and traffic engineering.

Dr. K. K. Ramakrishnan is a Technology Leader at AT&T Labs.- Research in Florham Park, New Jersey. He joined AT&T Bell Labs in 1994 and has been with AT&T Labs. Research since its inception in 1996. Between 2000 and 2002, he was at TeraOptic Networks, Inc., as Founder and Vice President. Prior to 1994, he was a Technical Director and Consulting Engineer in Networking at Digital Equipment Corporation. At AT&T Labs. Research, he is involved in several technical and strategic activities in networking, including Quality of Service, Congestion Control, Signaling, VPNs, IP Telephony and Metro Area Networks.

Shivkumar Kalyanaraman is a Professor at the Department of Electrical, Computer and Systems Engineering at Rensselaer Polytechnic Institute in Troy, NY. He holds a Computer Science B.Tech degree from IIT, Madras, India, and M.S., Ph.D. degrees from Ohio State University. His research interests include various traffic management topics and protocols for emerging tetherless networks. He is a member of the ACM and IEEE.