Design of Statistical-QoS VPN in IP Networks

Hoon Lee* and Yoon Uh* *Regular Members*

ABSTRACT

In this paper the authors propose a theoretic framework to design the Virtual Private Network (VPN) via which the Quality of Services (QoSs) are guaranteed over IP networks. The required QoS is a very strict packet loss probability or a probability that packet delay does not exceed a certain target value in a statistical manner. QoSs are guaranteed by providing a statistical bandwidth similar to equivalent bandwidth, which is computed so that the provided bandwidth is sufficient to guarantee those requirements. Two typical network architectures are considered in constructing VPN, the customer pipe scheme and the Hose scheme, and we propose a method to compute the amount of the required bandwidth for the two schemes. Finally, we investigate the implication of the scheme via numerical experiments.

I. Introduction

Recently, the electronic exchanges of documents and data inside and/or outside the enterprise network have become usual events, and as such the requirements for the connections between LANs have been extended to a distributed wide area network. At the same time, the development in the network technologies made it possible to use the ATM (Asynchronous Transfer Mode) or IP (Internet Protocol) networks as a part of the enterprise network. In this respect, the traditional private leased lines are likely to be replaced by VPN due to high capacity and reasonable price as well as satisfactory performance, and thus VPN is becoming an increasingly important source of revenue for the Information Service Providers (ISPs).

There exist plenty of issues concerning the design of the VPN. To name a few, we have to consider the security, pricing, network topology and resource dimensioning. Among them, the resource dimensioning, especially the bandwidth dimensioning with QoS-guarantee, is one of the key issues in order to secure satisfactory services to the users, because the goal of VPN is to provide end users with a service comparable to a private dedicated network established with leased lines.

In this paper, we focus on the issue of dimensioning the bandwidth for the VPN from the view point of guaranteeing the strict QoS of data loss, especially the packet loss rate of the data, and delay in statistical manner.

To the best knowledge of authors, there exist a few literatures that deal quantitatively with the bandwidth dimensioning of VPN from the viewpoint of statistical-QoS guarantee. Duffield proposed a capacity management scheme for the IP-VPN under the two connection schemes, the customer-pipe model and the hose model, which is applied to our VPN topology[3]. Those architectures are also discussed in [4] as an ATM version of VPN in the name of end-to-end VPN and the broadband VPN, respectively. However, neither has considered the QoS guarantee such as packet loss rate or delay. Anerousis proposed a dynamic dimensioning method for VPN using the concept of connection-oriented network with call blocking. However, the packet level QoS is not taken into account[2].

Our work is different from the previous works in the following points: First, in this paper, we

* Dept. of Information and Communication Engineering, Changwon National University
논문번호 : 010334-1115, 접수일자 : 2001년 11월 15일

assume the topologies described in [3], but we take into account the packet loss probability (PLP) or delay bound in the dimensioning of the required bandwidth for the packet network including the ATM or IP networks. Second, we assumed the long- range dependent traffic as an aggregated source from a customer network, which is considered to be the most typical source traffic environment in the real field. Third, via a simple approximate formula for the packet loss probability or the upper bound on the delay, we determine the required bandwidth capacity for each customer network under the assumed connection topology. Note that, for the simplicity in the description of the mathematical basis, we assume the IP network with fixed length packet.

This paper is composed as follows: In Section 2 we describe the VPN architecture. In Section 3 we propose a method for dimensioning the bandwidth capacity assuming the typical long-range dependent traffic. In Section 4 we present results of the numerical experiments. Finally in Section 5, we discuss implication of the work and summarize the work.

Ⅱ. VPN Architectures and Motivation for Statistical Bandwidth

Consider a distributed work environment of a company composed of headquarters in area A, three branch offices located at B, C and D, and assume that each site has LAN and they want to connect one another. Exchanges of information such as an e-mail or ftp are carried out between the members of different departments. The company can build a closed intra-network via VPN. Fig.1 illustrates a schematic diagram for the VPN environment.

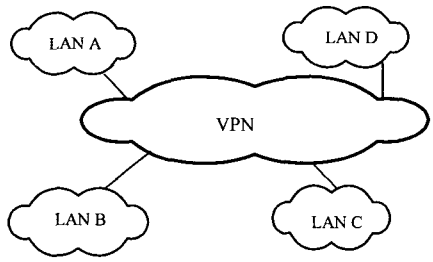


Fig.1. A diagram for VPN

Each site may have a specific attribute in the generation of traffic. However, this work assumes a total traffic aggregated from each site to the other sites, and they result in a general bursty traffic. It is usually known that the usage rate of leased-line or VPN is smaller than the contracted link speed. To illustrate our argument, Fig.2 shows usage rates of KORNET VPN. The data are obtained by averaging the peak rate of each day (traffic selected from busy hour) over a period of a year [7].

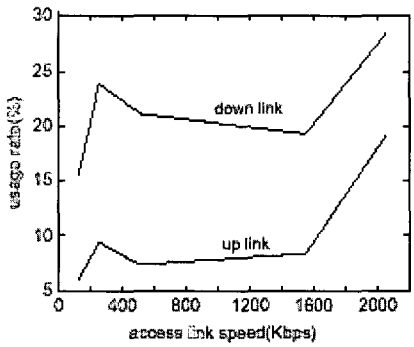


Fig. 2. Usage rate for KORNET-VPN.

As we can find from the Fig.2, the average usage rates of VPN users, which is defined to be the actually used rate divided by the link speed, for up and down links are low (ranging over 10 to 30% of the peak access link speed). This indicates that the usage rate of the core link of the VPN is low, too.

Therefore, there exist two possibilities in provisioning the bandwidth in the core:

(a) Overprovision the core link with peak rate and do not care about QoSs,

(b) Estimate the QoS requirements, and provide a statistical bandwidth, which is smaller than the peak rate.

In the previous research, the authors have identified that the latter approach is more favorable to the network operators because the approach (a) is too non-economical as we can see in Fig.2. Therefore, this work focuses on the estimation of bandwidth with statistical QoS

requirements, which is based on the latter approach

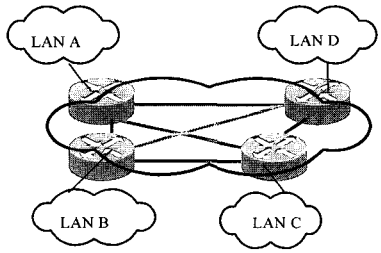
There exist two typical methods for constructing the VPN: the Customer Pipe -VPN scheme (or Pipe-VPN, we use the Pipe-VPN in the following) and the Hose-VPN scheme [3]. In Pipe-VPN, the physical network composed of the concatenation of nodes and links is mapped into a logical network, where each office is connected with the other offices by full-mesh of the nodes that inter-connect the offices in each area. This network architecture is usually shown in point-to-point services and is called to be a Pipe-VPN because each customer in VPN is connected to the other customers with a direct pipe like personal pipe between two end users. A path is created by a tunnel in IP network. This approach is favorable to the connections with known traffic distribution, so that the network operator can guarantee a quantitative QoSs for each route.

In Hose-VPN, end-to-end paths with the same directions are packed into an aggregated big pipe, and they are distributed after that. This approach assumes unknown traffic distribution from a group of customers, which is considered to be most attractive from the network operators' point of views. However, the resource has to be provisioned using prediction of the traffic based on historical patterns or some means of estimation. For the purpose of bandwidth design of LAN interconnections between sites via VPN, the assumption of statistical QoS guarantee is more suited to the transactions of aggregate traffic of IP network.

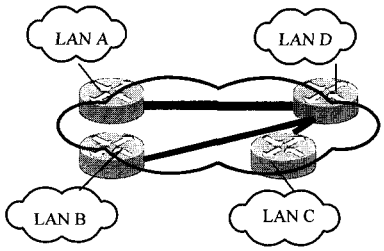
On the other hand, this approach results in much higher statistical multiplexing effect than that by Pipe-VPN scheme via bandwidth sharing. Note that the routing of each path is fixed and there exists only one path from a source to a destination.

Each scheme has pros and cons: The Pipe-VPN guarantees the QoS to each source-destination pair more strictly than the Hose-VPN at the expense of dedication of a path to each pair. However, as described in the above discussion, the network operator has to know the traffic matrix between all the VPN sites a priori, which is very difficult unless almost impossible to predict traffic characteristics between pairs of endpoints. In addition, the connections other than a specific connection from an area can not utilize the vacant bandwidth not used by a certain path.

On the other hand, the Hose-VPN can obtain much higher statistical multiplexing effect by aggregating the traffic with the same direction. The Hose-VPN requires no traffic matrix between all the VPN sites. So, the network operator has to know just the aggregated incoming and outgoing traffic for a certain node. Fig.3 (a) and (b) illustrates the Pipe and Hose VPN, respectively.



(a) Pipe-VPN



(b) Hose-VPN

Fig. 3. Pipe and Hose VPNs.

From this discussion, it follows that the Hose-VPN provides customers with a simple mechanism for specifying bandwidth requirements and enables VPN service providers to utilize network resources more efficiently, as discussed qualitatively in [9]. In the following sections we will give a quantitative background of the authors' argument in the support of the Hose-VPN as a more efficient way for IP-VPN.

Ⅲ. Bandwidth Dimensioning

The bandwidth corresponds to the capacity of links between the two routers in IP network, and there exist lots of approach for dimensioning bandwidth capacity [13]: Peak rate dimensioning, mean rate dimensioning or some rate between those two values such as the effective rate.

One more approach is the QoS-free algorithm that tries to slightly over-provide the bandwidth and avoid the complexity and costly congestion control [5]. From our viewpoint, the QoS-free concept can be suitable for the dimensioning of the backbone network where the information about the individual traffic profile is abstract and the traffic is smoothed by aggregating a large number of connections. Also, that approach can be applied to the dimensioning of the access link of the VPN on which our discussion is based. However, with QoS-free scheme, no QoS requirement is taken into account in the design of the bandwidth. In this paper, we propose a method to quantify bandwidth which is required to guarantee the statistical SLRs (Service Level Requirements) such as packet loss probability (PLP) and probability that packet delay does not exceed a certain value in the context of the asymptotic approximation by using the large deviation theory (LDT), the result of which corresponds to the equivalent bandwidth or the sustainable rate in the ATM network.

Let us assume that the aggregated traffic from an office i is served by a link with capacity Ci. The messages are segmented into a fixed-size packet, which begins to gain persuasive power considering the current trend in the usage-based charging levied by the number of packet transferred. Let us assume that the time scale for the transmission of a packet in the network is so small that the stream of packet is regarded as a fluid by the network. From the traffic trace of KT R&D center, it is known that the input and output traffic show self-similar characteristics where the Hurst parameter H is in the range of $0.5 < H < 1$, which illustrates that the LAN traffic has LRD (Long Range Dependent) over long time scale [12]. However, let us assume that the offered load between the offices are moderate or lightly loaded (From our experiments in KORNET, the KT's public IP network, the average usage rate of the access link for the IP-VPN is about 20% for a diverse access speed types) [6], so that the node congestion can be regarded as a very rare event, which enabled us to use the LDT. However, because we assumed that the traffic is very bursty in a short time scale, packet buffering at the node is inevitable.

In order to continue our discussion to the dimensioning of the required bandwidth for the link, let us assume as follows: The user does not have sufficient information for his/her traffic. The customer abstractly knows that he/she needs a certain level of mean rate and he/she requires that the ceiling of PLP or delay requirement such that their traffic meets the requirements up to a certain limit. On the other hand, let us assume that the network operator can measure mean and variance of the packet arrival rate and the PLP. The variance here is needed to accurately estimate the variation of the user's traffic from the mean rate.

Under the above-mentioned environment, let us determine the bandwidth between the nodes connecting the customer sites. Following the discussion of Li [10] and the assumption of fluid flow of the packet input-output, let A(t) be the number of arrivals generated by aggregated customers of the same branch office in the interval (0,t), which is given by

$$A(t) = \lambda t - \sigma Z(t) \tag{1}$$

where λ and σ is the mean and standard deviation of the packet generation rate, respectively, and Z(t) is normalized fractional Brownian motion with zero mean and variance equal to t^{2H}, H is the Hurst parameter (More on the Hurst parameter, refer to [11]).

If we assume that at most C packets can be served in a time interval, and if we let V(t) be

the number of packets in the buffer of infinite size, then we have the following formula for the remaining packet in the buffer at time t:

$$V(t) = \mathrm{Sup}_{s \le t}\{A(t)-A(s)-C(t-s)\} \quad (2)$$

3.1. Bandwidth for loss guarantee

In reality, the buffer size in a node is finite, as such we have to approximate the infinite buffer system into a finite buffer system. Let us define that the buffer overflow event for a finite buffer system with buffer size B is equivalent to the event that the buffer occupancy level V(t) in an infinite buffer system exceeds B, and let its probability be ϕ, which is represented as follows:

$$\Pr\{V(t) > B\} < \phi \quad (3)$$

The left hand side of the formula (3) can be rewritten as

$$\Pr\{V(t) > B\} = \Pr\{\mathrm{Sup}_{t>0}(A(t) - C_L t) > B\} \quad (4)$$

where C_L is the link capacity required to guarantee the statistical packet loss SLR, which is a special value of C in eq. (2). Note that eq. (4) reduces to

$$\Pr V(t) > B = \mathrm{Max}_{t>0}(\Pr A(t) > C_L t + B) \quad (5)$$

If we assume that the traffic coming into an access node of VPN is aggregated by a large number of populations, we can assume that the aggregated input process to each access node follows a Gaussian distribution. From the argument in [1], we obtain the following formula:

$$\Pr\{A(t) > C_L t + B\}$$
$$\exp\{-(C_L-)^{2H} B^{2-2H}/(2^2((1-H)^{1-H}H^H)^2)\} \quad (6)$$

From (3) and (6), we obtain a formula for the amount of the bandwidth required to guarantee PLP ϕ which is given as follows:

$$C_L = \lambda + (\frac{-\log\phi}{K_L})^{\frac{1}{2H}} \quad (7)$$

where K_L in eq. (7) is given by

$$K_L = \frac{B^{2-2H}}{2\sigma^2((1-H)^{1-H}H^H)^2}. \quad (8)$$

From the formula (7) one can find that the required bandwidth for guaranteeing VPN traffic with PLP requirement is greater than the mean bit rate declared by a connection in an amount equivalent to the second item in the RHS of the formula (7). Note that the additionally required bandwidth depends on the variance of the arrival rate and the Hurst parameter as well as the required PLP under the given buffer size.

3.2. Bandwidth for delay guarantee

The required bandwidth for the statistical delay guarantee can be derived in a similar manner that we have obtained the formula (7). Let W(t) be the delay in the buffer at time t and let C_D be the required bandwidth for the delay guarantee. Since we have assumed a fixed packet length, the delay W(t) is simply given by

$$W(t) = \frac{V(t)}{C_D} \quad (9)$$

Let the delay requirement be defined to be

$$\Pr\{W(t) > \tau\} < \varphi \quad (10)$$

where τ is the target end-to-end delay and φ is the upper bound of the delay-violation probability. If we reduce the end-to-end delay into a nodal one, which is denoted by τ_n,
Then, eq.(10) reduces to

$$\Pr\{V(t) > C_D\tau_n\} < \varphi \quad (11)$$

Comparing the two inequalities (3) and (11), one can find that a formula for the minimum value for the required bandwidth C_D is given as follows:

$$C_D = \lambda + (\frac{-\log\varphi}{K_D})^{\frac{1}{2H}} \quad (12)$$

where K_D is given by

$$K_D = \frac{(C_D \tau_n)^{2-2H}}{2\sigma^2((1-H)^{1-H} H^H)^2}. \quad (13)$$

Note from eq.(13) that K_D is also a function of C_D, so eq.(12) is numerically computed using the standard root-finding method.

After we obtain the required bandwidths for the loss and delay guarantee in the VPN we can choose values C for a specific QoS objectives such that $C=C_L$ for connections with packet loss requirement only, $C=C_D$ for connections with packet delay requirement only, and

$$C = \mathrm{Max}[C_L, C_D] \quad (14)$$

for a connection with both packet loss and delay requirements. One can assume that it is not always necessary for an application to require guarantee of both requirements. Applications with tight delay limit will be provided with a bandwidth amount of C_D, whereas applications with tight packet loss requirement will be provided with a bandwidth amount of the C_L as a target bandwidth. Therefore, simple comparison of those two values of C_D and C_L does not have a physical meaning. Therefore, we will illustrate the result of numerical experiment for both cases separately.

Ⅳ. Numerical Experiments

Let us illustrate a design example for the proposed method. First, let us assume that a backbone network supports the VPN by constructing a path similar to ATM's PVC (Permanent Virtual Circuit). Thus, the network uses the fixed routing algorithm such as shortest path selection between the source and destination nodes. Table 1 shows the traffic matrix between the source-destination pair for each end-to-end office, which corresponds to the end-to-end traffic matrix between the CP-VPN architecture by arbitrarily assuming the weight in the amount of the data transactions between the Headquarters and the branch offices. The link speed of the access line is assumed to be T1 with 1.544Mbps. The average load in each item for Table 1 is chosen arbitrarily. However, we tried to be realistic in choosing those values by taking into account the real trend of KORNET-VPN traffic data as we have shown in Fig.2, where the average usage rate of a customer ranges about 10 to 30% of the contracted rate. In Table 1, a minimum offered load of 0.2Mbps corresponds to a usage rate of 13% of link capacity and a maximum offered load of 0.7Mbps corresponds to a usage rate of 45.3% of link capacity. Therefore, the assumptions on the traffic load in Table 1 are sufficiently realistic.

Table 1. Traffic matrix for Pipes [unit: Mbps]

	A	D	B	C
A	×	0.7	0.3	0.4
D	0.7	×	0.3	0.2
B	0.3	0.3	×	0.3
C	0.4	0.2	0.3	×

In Table 1, a notation (implies that the traffic inside the same location is out of the consideration in dimensioning the VPN. For simplicity we assumed that the traffic is symmetric (say, traffic from node A to node B is equal to the traffic from node B to node A). A case for non-symmetric case is trivial. Table 2 represents the traffic matrix of the Hose-VPN for the traffic load assumed in Table 1. For example, the traffic load of the link between the nodes A and D for the Hose-VPN is sum of the traffic between the node pairs A-D, A-B and A-C.

Table 2. Traffic matrix for Hoses [unit: Mbps]

	A	D	B	C
A	×	1.4	×	×
D	1.4	×	0.9	0.9
B	×	0.9	×	×
C	×	0.9	×	×

Note that the aggregated traffic 1.4Mbps between sites A and D in Table 2 corresponds to 90.67% of the link speed T1 of an access link. Therefore, we can easily find that all the paths in

a network can cope with the load with only one T1 link if there exists no requirement for the packet loss or delay guarantee even though the backbone network provides the VPN users with a mean valued bandwidth dimensioning.

4.1. Bandwidths for loss guarantee

First, let us compute the bandwidths of the links for the Pipe-VPN. The end-to-end PLP requirements for all the paths are assumed to be 10^{-12}, and buffer is provided for each originating node and buffer size is assumed to be 1000 packets. For the simplicity of calculation, let us assume that the variance is ten times the mean value, viz. $\sigma^2=10\lambda$, for all traffic and Hurst parameter is assumed to be 0.8.

Table 3 illustrates the results for the bandwidth between the source-destination pair of the Pipe-VPN architecture. Note that the network operators have to provide a bandwidth much greater than the mean source traffic rate in order to guarantee a very strict PLP requirement of 10^{-12}. In case of the source-destination pair A-D in Table 3, the required bandwidth is about seven times that of the mean source traffic rate.

Table 3. Bandwidth matrix for Pipes [unit: Mbps]

	A	D	B	C
A	×	4.64	2.62	3.18
D	4.64	×	2.62	2.00
B	2.62	2.62	×	2.62
C	3.18	2.00	2.62	×

This trend is shown in all the links. These results come mainly from the strictness in the PLP requirements.

Table 4. Bandwidth matrix for Hoses [unit: Mbps]

	A	D	B	C
A	×	6.02	×	×
D	6.02	×	4.40	4.40
B	×	4.40	×	×
C	×	4.40	×	×

Table 4 illustrates the bandwidth between the neighboring nodes for the Hose-VPN under the same conditions that have been assumed in computing Table 3. We assumed the same parameters as with Table 3 except that the buffer size prepared for aggregated traffic is summed up to be 3000.

Let us compare the Tables 3 and 4. Consider the total output link at the node A. The total required bandwidth of the output link of the node A under the Pipe-VPN architecture is 10.44Mbps, whereas the Hose-VPN requires only 6.02Mbps, saving 42.3% of the bandwidth.

Now, let us compare the total bandwidth required to provide the VPN for the company. The total one-way bandwidth for the Pipe scheme and Hose scheme is 17.68 Mbps and 14.82 Mbps, respectively. Thus, the Hose scheme can save about 16.3% of the bandwidth.

4.2. Bandwidths for delay guarantee

Let us compute the bandwidths of the links necessary to guarantee a limited delay to delay-sensitive connections. To that purpose, let us assume that the application used is a telephony service. It is known from experiments that the end-to-end packet delay requirement for the typical voice should not exceed 150ms for good quality, which is classified as a class 0 for IP networks that is to be achieved on the complex 27,500Km hypothetical reference paths [8]. If this class 0 is assumed in the national network, this requirement is very conservative. Therefore, let us assume a target end-to-end delay limit to be 100msec.

If we assume an evenly distributed delay along the network, which is typical for the well designed network, and if we know the number of node along the path for a specific connection, which is usual in VPN, and let it be N, we can represent the delay that a packet experiences in a node in the following way:

$$\tau_n = \frac{\tau}{N}. \tag{15}$$

Let us assume that N=10, which is the typical

value for the average number of node a packet passes along a path in a continent. However, N will vary depending on the scale of network associated with the end-to-end path. Let us assume that a sufficient capacity of buffer is provided for each node and buffer size is assumed to be infinite. The source traffic parameters are assumed to be the same as we have described in Section 4.1 except that the Hurst parameter has been assumed to be 0.5 for computational simplicity (a source is said to be self-similar if the Hurst parameter is not less than 0.5 and not greater than 1).

Table 5 illustrates the results for the bandwidth between the source-destination pair of the Pipe-VPN architecture. Note that the network operators have to provide a bandwidth much greater than the mean source traffic rate in order to guarantee a packet delay requirement of 100ms end-to-end, which has been found in the previous experiment for loss requirement, too. For example, in case of the source-destination pair A-D in Table 5, the required bandwidth is about six times that of the mean source traffic rate.

Table 5. Bandwidth matrix for Pipes [unit: Mbps]

×	A	D	B	C
A	×	4.01	3.11	3.38
D	4.01	×	3.11	2.77
B	3.11	3.11	×	3.11
C	3.38	2.77	3.11	×

Table 6 illustrates the bandwidth between the neighboring nodes for the Hose-VPN under the same conditions that have been assumed in computing Table 5.

Table 6. Bandwidth matrix for Hoses [unit: Mbps]

	A	D	B	C
A	×	5.07	×	×
D	5.07	X	4.35	4.35
B	×	4.35	×	×
C	×	4.35	×	×

Let us compare the Tables 5 and 6. Consider the total output link at the node A. The total required bandwidth of the output link of the node A under the Pipe-VPN architecture is 10.5Mbps, whereas the Hose-VPN requires only 5.07Mbps, saving 51.7% of the bandwidth. The saving of bandwidth can be found for all the links in the network, so that we can conclude that the Hose-VPN is assumed to be more economic than the Pipe-VPN.

4.3. Remarks

Summarizing the above results, we can find that the Hose-VPN scheme is more favorable than the Pipe-VPN scheme from the two viewpoints. First, the Hose-VPN scheme requires less total bandwidth capacity than the Pipe-VPN scheme due to statistical multiplexing gain obtained by traffic aggregation. Second, the Hose-VPN scheme aggregates the separate connections in the Pipe-VPN scheme in a fat pipe, so that it is easy for the network operator to specify the traffic requirements and to manage the network resources, because the statistical variability in the individual source-destination traffic is smoothed by aggregation into hoses.

V. Conclusions

In this paper, we proposed a method for dimensioning the bandwidth required for guaranteeing the strict but statistical PLP or packet delay requirements in the VPN over the broadband IP networks. We assumed two typical VPN topologies: the Pipe-VPN and Hose-VPN. Via analytical methods we derived bandwidths required to guarantee specified packet loss rate or upper bound on the delay using the asymptotic approximation of the long-range traffic that is inherent to the current data networks.

From the numerical experiments of a network consisting of a series of nodes, we could verify the superiority of the Hose-VPN model compared to the Pipe-VPN model from the economic point of view. The results presented in this paper may be utilized as means to the bandwidth design of

VPN networks.

References

[1] R.G. Addie, "On the applicability and utility of Gaussian models for broadband traffic", Faculty of Sciences, USQ, Working Paper Series SC-MC-9815.

[2] N. Anerousis, "Dynamic virtual network dimensioning in cost-sensitive environments", Proceedings of Globecom'99, 1999.

[3] N.G. Duffield, P. Goyal and A. Greenberg, "A Flexible model for resource management in Virtual Private Networks", ACM SIGCOMM '99.

[4] S. Fotedar, et.al., "ATM virtual private networks", Communications of ACM, Vol.38, No.2, February 1995.

[5] H. Hosogoezawa, S. Yoneda and T. Aoki, "An IP network design rule to meet QoS demands of users", Technical Report of IEICE CS99-153(2000-02).

[6] H. Lee, J.H. Eom and Y.C. Baek, "A Usage-Rate Based Charging for QoS-Free Traffic in IP-VPN", KT Journal, Vol.6, No.3, December 2001.

[7] H. Lee, et. al., "Estimation of generated traffic for the KORNET leased-line users", Internal Report of KT Telecommunications Network Lab., June 2000.

[8] Revised draft Recommendation Y.1541, "Internet protocol communication services-IP performance and availability objectives and allocations", Temporary document (WP4/13), Q.13, ITU-T, November 20-24, 2000.

[9] Amit Kumar, "Algorithms for provisioning VPNs in the Hose model", ACM SIGCOMM '01, August 27-31, 2001, San Diego, California USA.

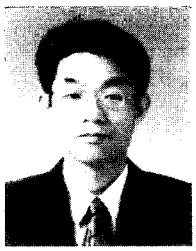
[10] J-S Li, "Measurement and in-service monitoring for QoS violations and spare capacity estimations in ATM network", Computer Communications, 23(2000).

[11] Z. Sahinoglu and S. Tekinay, "On multimedia networks: Self-similar traffic and network performance", IEEE Communications Magazine, January 1999.

[12] S.M. Yang, "Fractal characteristics in KORNET traffic", Korea Telecom TM, 1999.

[13] H. Yokoi and T. Tsuchiya, "VP bandwidth design based on estimation of queue length distribution in a buffer", Technical Report of IEICE SSE99-16 (1999-05).

Hoon Lee



He received the B.E. degree in Electronics and M.E. degree in Communications from Kyungbook National University, Daegu, Korea, in 1984 and 1986, respectively. He received the Ph.D. degree in Electrical and Communication Engineering from Tohoku University, Sendai, Japan, in March 1996.

From February 1986 to February 2001, he worked at KT, Telecommunications Network Lab., where he has been engaged in the research on the teletraffic engineering, network design, performance analysis of telecommunication networks. He is currently an Assistant Professor of Changwon National University, from March 2001. His current research interests include network design, performance analysis and provision of QoS for high speed telecommunication networks. Dr. Lee is a member of IEEE, KICS and IEEK.

Yoon Uh

He received the B.E. and M.E. degrees from Hanyang University, 1982 and 1986, respectively. He received the Ph.D. from Tohoku University, Sendai, Japan, 1994. From January 1986 to July 1987 he worked at LG Electric, LTD. From September 1987 to June 1998, he worked at ETRI as a senior research staff.

From September 1998, he is an Assistant Professor of Changwon National University. His research interests include digital communication systems and coding theory. Dr. Uh is a member of IEEE, KICS and IEEK.