QoS Routing for IP-based Virtual Private Network Services*

L.Huan[1], O.Kabranov[1], L.Orozco-Barbosa[1,2], D.Makrakis[1]

[1]School of Information Technology and Engineering
University of Ottawa, 161 Louis Pasteur, Ottawa, ON, K1N 6N5 Canada
[hliang, kabranov, lorozco, dimitris]@site.uottawa.ca

[2]Instituto de Investigación en Informática, Universidad de Castilla La Mancha
Campus Universitario, Albacete 02071 SPAIN
Luis.Orozco@uclm.es

Abstract
IP-based VPN technology is considered an attractive cost-effective private network service for both customers and service providers. We focus our research on the design of a minimal cost routing policy to be used by network-based IP VPN. The interest in such solutions is generated by both customers seeking to reduce support costs and by Internet Service Providers (ISPs) seeking new revenue sources. Reducing the cost of operation would allow ISPs to define and deploy new VPN services.

In particular, a Multi-commodity Min-Cost Flows (MMCF) formulation is applied to the resource allocation in network-based IP VPN in order to develop a cost-effective routing proposal. We compare our proposal with the IETF RFC 2676 enhancement : a QoS enhancement to the Open Shortest Path First (OSPF) algorithm. Our results show the benefits of our proposal by considering two different scenarios.

1. Introduction

A private network could be understood as an Intranet supporting services, such as electronic mail, web surfing, database and groupware to authorized users [1]. In the 1990s, private networking services were widely used to deploy intranet services. According to the Open Systems Interconnection (OSI) model, VPN solutions can be classified as Layer 2-based approaches, e.g. Frame Relay or ATM-based VPN, and Layer 3-based approaches, e.g. Multiple Protocol Label Switch (MPLS) VPN and Internet Protocol (IP) VPN[2][3][4][5]. Depending on the application scenario, they all have their individual advantages and drawbacks. For instance, a Frame Relay VPN is considered inherently secure due to the fact that uses layer 2 technologies but it is considerable more expensive than IP. On the other hand, MPLS VPN is a layer 3-based technology and therefore substantially more scalable. However, it requires that all sites be tied into the same service provider and therefore it does not lend itself to remote access from remote dialup users. IP VPN is cheaper, easy to build and have a clear advantage in remote access applications. In addition, the latency of IP connections is expected to improve [1]. However, among the existing solutions, IP VPN is a good choice in terms of costs and independence from the underlying communication infrastructure. Nowadays, more and more research and development efforts focus on IP VPN service solutions.

Our research focuses on IP-based VPNs, where the operation of a VPN is outsourced to an Internet Service Provider (ISP). It is now recognized that solving the cost minimization would allow Internet Service Providers to define and deploy new VPN services [1]. Our main objective is the definition of a Multicommodity Min-Cost Flows (MMCF) routing policy to address the optimal resource allocation in a network-based IP VPN. Accordingly, a minimal cost VPN tunnel is proposed by using the network flow optimization based to define a cost-effective network management system. From the point of view of the service provider, MMCF proves effective by minimizing the cost of the network operation. The main novelty of our proposal comes from the fact that the costs involved in the transport are addressed as a part of the routing metric.

In the following the paper is organized. Section reviews the principles of the RFC 2676 - Open Shortest Path First (OSPF), one of the IETF standards OSPF and introduces our proposal. Section 3 describes the scenarios used in our performance study. Section 4 shows our numerical results. Section 5 draws our conclusions.

2. QoS ROUTING

2.1. OSPF – Routing and QoS Principles

OSPF is an industry standard protocol developed by the Internet Engineering Task Force (IETF). Basically OSPF is a Shortest Path First (SPF) algorithm. As a link state routing protocol [6], OSPF maintains a topological

* This work has been partially supported by the Natural Science and Engineering Research Council of Canada (NSERC).

database, which stores related information of the autonomous network state and uses it to calculate the shortest path. Link-state information is exchanged in the form of LSA (link-state advertisements). According to the OSPF version 2 in RFC 2328, LSAs are exchanged every 30 minutes, unless there is a change in the network topology. To apply QoS mechanism to the network, an experimental protocol – "QoS Routing Mechanisms and OSPF Extensions" RFC 2676 has been developed.

The focus of RFC 2676 is on the algorithms used to compute QoS routes and on the necessary modifications to OSPF to support this function. The purpose of RFC 2676 is to identify possible approaches to allow the deployment of QoS routing capabilities with the minimum possible impact to the existing routing infrastructure. The assumptions of RFC 2676 are the following: 1) QoS-capable routers in the network are assumed to identify and advertise resources that remain available to new QoS flows, 2) Hop-by-hop path selection model is discussed in RFC 2676, 3) Path selection is itself limited to considering only bandwidth requirements. In particular, the path selection algorithm selects paths capable of satisfying the bandwidth requirement of flows, while at the same time tries to minimize the amount of network resources that need to be allocated, i.e., minimizes the number of hops used. In RFC 2676, the path selection information and algorithms are explained as follows.

The process of selecting a path that can satisfy the QoS requirements of a new flow relies on both the knowledge of the flow's requirements and characteristics, and information regarding the availability of network resources. Accounting for these aspects, path selection involves the following metrics: 1) link available bandwidth, 2) link propagation delay; and 3) hop-count: this quantity is used as a measure of the path costs to the destinations. A path with a smaller number of hops (that can support a requested connection) is preferable since it consumes fewer network resources.

It is assumed that each router maintains an updated database of the network topology, including the current state (available bandwidth and propagation delay) of each link. In addition to the distribution of link state information, another important aspect is the time that such distribution takes.

There are two main options to implement the algorithm. One is to perform on-demand computations, that is, trigger a computation for each new request. The other is to use some form of pre-computation. RFC 2676 primarily focus on the case of pre-computed paths, which is also the only method currently supported in the reference implementation. The OSPF 2676 design objectives are to support for path pre-computation with hop-by-hop routing. The scope of QoS route computation is currently limited to a single domain. All routers within a domain are assumed to run a QoS enabled version of OSPF, i.e., inter-operability with non-QoS aware versions of the OSPF protocol is not considered.

2.2. Our Proposal

As previously mentioned, the research focuses on the minimal cost design suitable for a network-based IP VPN service provider. According to the current market trends, IP VPN billing is applied to basic service fee charges for Customer Premises Equipment, site-to-site connectivity, end-to-end management and monitoring. In this way, a site within a VPN receives a monthly bill based on access speed (bandwidth). These fees apply for VPN customers and they are flexible due to the market competition. Therefore, if a service provider expects to survive in the price competition and maximize its revenue, one of the options is to reduce the cost of connectivity. In other words, by optimizing the routing algorithm the lowest cost path is selected for the VPN customer and at the same time, the SLA requirements are respected. Towards this end, the Multicommodity Min-Cost Formulation (MMCF) is proposed. The purpose of min-cost flow is to minimize the total cost subject to availability and demand at some nodes and upper bound the flow through each link [7].

Consider a directed network with N nodes and K links (commodities). The decision variables are x_{ij}, the flow through a link (formally represented by an arc) is represented by arc (i,j). The given information includes: c_{ij}: cost per unit of flow from node i to node j, u_{ij}: capacity (or upper bound) on flow from i to j, b_i: net flow generated at i. This latter follows the sign convention: $b_i > 0$ if n_i is a supply node, $b_i < 0$ if n_i is a demand node and $b_i = 0$ if n_i is a transit node. The main objective is to minimize the total cost of sending the supply through the network to satisfy the demand. The linear programming formulation for this problem is:

$$\text{Minimize } \sum\sum c_{ij}x_{ij}$$

$$\text{Subject to } \sum_j x_{ij} - \sum_j x_{ji} = b_i \text{ for all nodes}$$

$$0 < x_{ij} < u_{ij} \text{ for all arcs}(i,j)$$

Again, we will assume that the network is balanced, so $\sum_i b_i = 0$. Let the decision variables x^h_{ij} denote the flow of commodity *h* on *arc (i, j)* and c^h_{ij} be the per unit cost for commodity *h* on *arc (i, j)*. u_{ij} is the capacity (or upper bound) on flow from *i* to *j* and $u^h{}_{i,j}$ is capacity for commodity *h* on *arc(i,j)*; $b^h i$ is commodity net flow generated at node *i*. Using this notation we can formulate the Multicommodity Min-cost Flows problem (MMCF) as follows [1][7]:

We require to find the route of commodities on the directed network at minimal total cost, respecting the node balance constraints and individual (or single commodity) constraints $0 \le x^h_{ij} \le u^h{}_{i,j}$ *as well as the aggregate capacity constraints* $\sum_h x^h_{ij} = u_{ij}$. *So the following formulation of MMCF is used to match the network IP-based VPN design objective.*

$$\min \sum_{h \in K} \sum_{(i,j) \in A} c^h_{ij} \cdot x^h_{ij} \qquad (1)$$

$$\sum_{j:(i,j) \in A} x^h_{ij} - \sum_{j:(j,i) \in A} x^h_{ji} = b^h_i \quad \forall i \in N \qquad (2)$$

$$0 \le x^h_{ij} \le u^h_{ij} \quad \forall (i,j) \in A \qquad (3)$$

$$\sum_{h \in K} x^h_{ij} \le u_{ij} \quad \forall (i,j) \in A \qquad (4)$$

A. MMCF routing with bandwidth guarantees

Because each site within the VPN receives its monthly bill based on the access speed, bandwidth is the first QoS metric to be considered. In order to adjust our formulation to the QoS-enabled VPN service, we make the following assumptions: 1) the network links are bi-directional; 2) the capacity of the physical links are limited by an upper bound; 3) the SLA between ISP and end-customer is defined in terms of the reserved bandwidth for the virtual connection.

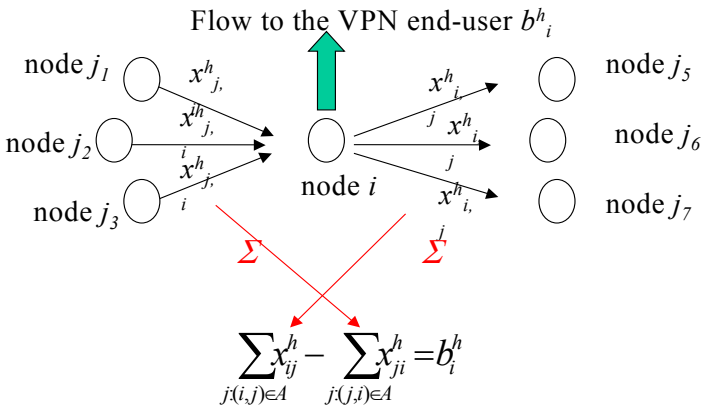


Figure 1. Equation (2) – flow conservation equation

Equation (1) represents the ISP total transport cost for operating the network while satisfying the VPN customer demands. c^h_{ij} is the allocation cost per bandwidth unit, belonging to virtual channel *h* on physical link *ij*. x^h_{ij} is the amount of allocated bandwidth belonging to virtual channel *h* on physical link *ij*.

Equation (2) is the flow balance equation for every node (see Figure 1). Inequality (3) is related to bi-directionality of the physical links.

The result of solving this optimization problem is the flow allocation x^h_{ij}. The allocation is the optimal routing - the amount of bandwidth, allocated for every virtual connection *h* on the corresponding physical link *(i,j)*.

B. MMCF with both bandwidth and delay considerations

Regarding the VPN delay requirement, real-time sensitive applications such as video and voice-over-IP (VoIP) are the most popular services to be considered. A commonly cited rule of thumb by VoIP vendors is that round-trip delay times for high-quality voice should be less than 150 ms. For these specific research models the one-way VPN required delay (named MAX_DELAY) is taking into consideration. Because the scalability of the physical model is much smaller than a transcontinental network running from San Francisco to Boston the MAX_DELAY should be much less than 21ms.

Let d^h_{ij} be the amount of accumulative delay, belonging to virtual channel h on physical link ij. Hereby, the accumulative delay for one-way VPN traffic must meet $\sum_{j:(i,j)\in A} d^h_{ij} \le MAX\_DELAY$ as well. The following formulation solves both bandwidth and delay considerations.

$$\min \sum_{h\in K}\sum_{(i,j)\in A} c^h_{ij}\cdot x^h_{ij} \qquad (6)$$

$$\sum_{j:(i,j)\in A} x^h_{ij} - \sum_{j:(j,i)\in A} x^h_{ji} = b^h_i \quad \forall i \in N \qquad (7)$$

$$0 \le x^h_{ij} \le u^h_{ij} \quad \forall (i,j)\in A \qquad (8)$$

$$\sum_{h\in K} x^h_{ij} \le u_{ij} \quad \forall (i,j)\in A \qquad (9)$$

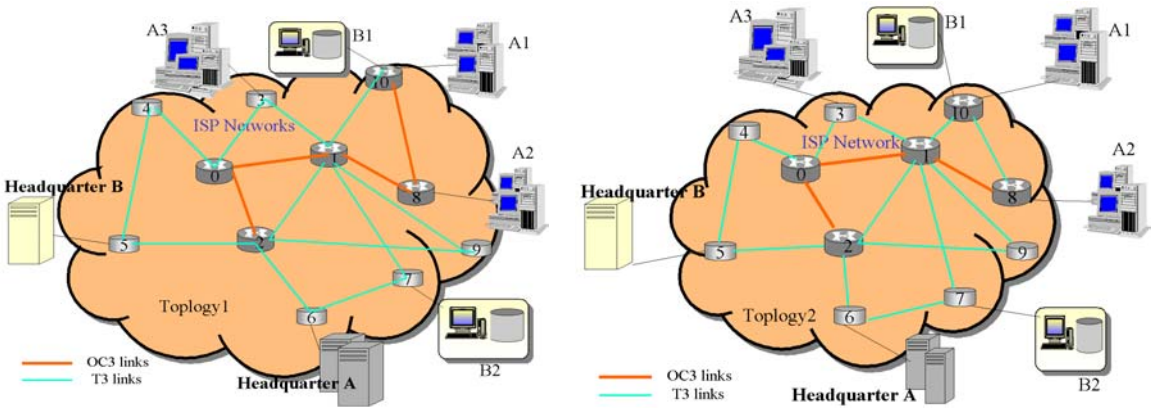
$$\sum_{j:(i,j)\in A} d^h_{ij} \le Max\_delay \quad \forall (i,j)\in A \qquad (10)$$

3. PERFORMANCE STUDY

3.1 Loading Conditions and network topologies

In the model developed in Section 2, there are two main data sources to take into account: 1) the VPN traffic in the service provider's network and 2) other (Internet) traffic. Currently, the VPN customers contract the service by specifying the required access speed, which is fixed. In other words, the VPN traffic does not have to be generated packet by packet. Instead, the VPN traffic can just be described by the amount of contracted bandwidth.

For the other Internet traffic, there are two approaches to describe the traffic. One option is to develop a traffic generator that can be built based on a mathematical model. The other option is to collect data from existing traffic traces taken from real networks. For the sake of simplicity and accuracy, the second option has been selected and applied in this study.



(a) (b)

Figure 2. Network Topologies a) Topology 1 b) Topology 2

Today, the ever-increasing Internet traffic is driving the Internet service providers (ISP) to analyze whether their network resources are sufficient enough to satisfy their customers. The previous traffic data collections just regarded some specific protocols or applications, which cannot reflect all current traffic through each ISP. It is therefore important to make use of more up-to-date traffic traces. One graceful resource is the WIDE (Widely Integrated Distributed Environment) project [9], which provides daily traffic trace data. Figure 2 depicts the two network topologies considered through our evaluations.

Topology 1 is composed of a total of four OC3 links and twelve T3 links. For the evaluation of this topology, we have used the WIDE OC3 traces of August 1st to August 4th (see [9] for details) to emulate the traffic over the four OC3 links of this topology. Similarly, we use the twelve WIDE T3 traces (August 1st to August 12th) for the T3 links. Specifically, we have used the traffic trace of August 1st to emulate the traffic flowing from node 0 to node 1; the traffic trace of August 2nd for the traffic flow from node 0 to node 2 and so on. Similarly, we have used the traffic traces to emulate the traffic for the T3 links.

In order to evaluate our system, we have run eight different experiments. For each link, we have used eight different time instants from the trace being used for that particular plot. For instance, for the OC3 link between node 0 and node 1, we have used the traffic trace of August 1st corresponding to the time instants 00:00, 03:00, 06:00…21:00. Based on the above traffic data figures and discussion, Tables 1 and 2 provide the details of the traffic used in Topology 1 in order to run the eight simulation cases.

Table 1. OC3-links traffic for network Topology 1

Simulation number	Initial Time	OC3 Internet Traffic data collection (Mbps)			
		August 1st	August 2nd	August 3rd	August 4th
1	00:00	13.2	95	3.5	4.2
2	03:00	6.5	63	8	17
3	06:00	5.4	2	3.8	1.5
4	09:00	94	3.5	7	1.3
5	12:00	96.5	13	8	3.5
6	15:00	21.5	17	24	4.7
7	18:00	9.8	8.5	12	8
8	21:00	5.5	5	11	18

Table 2. T3-links traffic for Topology 1

Simulation number	Initial time	T3 Internet Traffic data collection (Mbps)											
		8.01	8.02	8.03	8.04	8.05	8.06	8.07	8.08	8.09	8.10	8.11	8.12
1	00:00	16	12	2	9.5	15	14.2	15.8	12	10.4	10.2	7.2	8
2	03:00	13	10.8	9.8	13.6	14.2	19	12	9.8	9.2	11	9.3	7.2
3	06:00	8.8	7.2	10.6	9	9	9	8.7	10	12.8	22	7	4.4
4	09:00	9.8	12	9	8.3	14	10.5	9.2	10.4	11	5	4.2	11.8
5	12:00	22	17	8.5	10.8	19.8	23	12.8	12	9.4	8.6	7	9.5
6	15:00	14.5	16.2	16	11.2	23	17.5	20	15.8	13.2	9	12	10
7	18:00	18	16	9.5	15.1	21.6	17	19.7	20.1	17	8	9.9	10.8
8	21:00	11	13	14.3	12.2	17.3	12	13.8	14	11	9.2	11.2	8

Topology 2 has only three OC3 links instead of the four links of Topology 1. We have used the traffic data of the WIDE network of August 1st, 2nd and 3rd. (see Table 3). Besides, one extra T3 link replaces the OC3 link between node 8 and node 10 in Topology 2. So there are a total of 13 T3 links instead of 12. The traffic data of this link has been collected from the trace of August 13th 2002.

Table 3. OC3-links traffic data for Topology 2

Simulation number	Initial Time	OC3 Internet Traffic data collection (Mbps)		
		August 1st	August 2nd	August 3rd
1	00:00	13.2	95	3.5
2	03:00	6.5	63	8
3	06:00	5.4	2	3.8
4	09:00	94	3.5	7
5	12:00	96.5	13	8
6	15:00	21.5	17	24
7	18:00	9.8	8.5	12
8	21:00	5.5	5	11

3.2 Network Configuration

We have carried out several numerical computations for the two topologies under consideration. Table 4 depicts the network setup used for network Topology 1. The first column indicate the source and destination nodes. The second column shows the link capacity. If there is a direct link between the source and destination node, 45 Mbps is assigned for a T3 link and 155 Mbps for OC3 link. The following column indicates the bit rate of the Internet traffic other than the VPN traffic transiting over the link. The available bandwidth for the VPN traffic reported in Column 4 has been determined by subtracting from the link capacity the bit rate of the Internet traffic given in Column 2. The column labeled OSPF (Column 5) reports the remaining available bandwidth after having reserved the bandwidth required by the VPN service when using the OSPF routing protocol. Similarly Column 6 reports the bandwidth used when applying MMCF to reserve the bandwidth required by the VPN service. The last column is the service provider's cost information of each leased link, where $267 per Mbps is assigned for OC3 link traffic, $667 per Mbps for T3 link traffic.

Table 4. Partial link information for simulation number 5 – Bandwidth only

Nodes S-D	**Links**		**Available Bandwidth**			**Link Cost ($)**
	Capacity (Mbps)	**Load (Mbps)**	**Initial (Mbps)**	**OSPF (Mbps)**	**MMCF (Mbps)**	
0-1	155	96.5	58.5	58.5	40.5	267
0-2	155	13	142	142	107	267
0-3	45	22	23	15	15	667
0-4	45	17	28	28	28	667
1-0	155	96.5	58.5	58.5	23.5	267
1-2	45	8.5	36.5	1.5	36.5	667
1-3	45	10.8	34.2	34.2	34.2	667
1-7	45	19.8	25.2	12.2	12.2	667
1-8	155	8	147	142	142	267
1-9	45	23	22	22	22	667
1-10	45	12.8	32.2	32.2	32.2	667
2-0	155	13	142	134	116	267
2-1	45	8.5	36.5	18.5	36.5	667
2-5	45	12	33	18	18	667
2-6	45	9.4	35.6	15.6	15.6	667
2-9	45	8.6	36.4	36.4	36.4	667
3-0	45	22	23	23	23	667
3-1	45	10.8	34.2	34.2	34.2	667

4. NUMERICAL RESULTS

A. Results under bandwidth reservation

Figure 3 shows the results for the MMCF and OSPF schemes for both topologies. In the case of Topology 1, MMCF saves on average a 8.9% over the OSPF-based routing (RFC2676). In the case of Topology 2, on average, the MMCF protocol saves on average a 6.1% over OSPF (RFC2676).

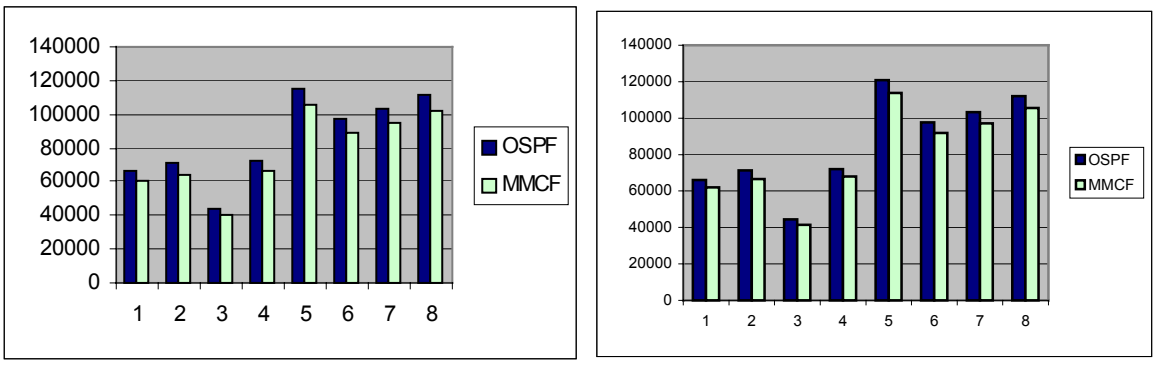


Figure 3. Numerical results a) Topology 1 b) Topology 2

According to our simulation results, the MMCF algorithm is effective on reducing the costs of a VPN service provider. Both methods meet the bandwidth requirement. The difference is that OSPF always selects the path with minimal hops and if the number of hops is the same, the path with more available bandwidth is selected. However, the MMCF scheme first finds the cheapest cost path for the VPN service and if the cost is the same then the path involving the minimum number of hops with more available bandwidth is chosen. It is the selection mechanism that makes the difference.

B. Results under bandwidth and delay constraints

Based on [8], one-way delay is considered here because in many Internet paths are asymmetric i.e., the sequence of routers traverse by a packet from a source to a destination may be different from the sequence traversed from the same destination back to the same source. The delay constraint MAX_DELAY is a constant threshold. In our analysis, MAX_DELAY is assumed to be 6 ms comparing with the 21 ms one-way delay of network. Each link's propagation delay is assumed as well.

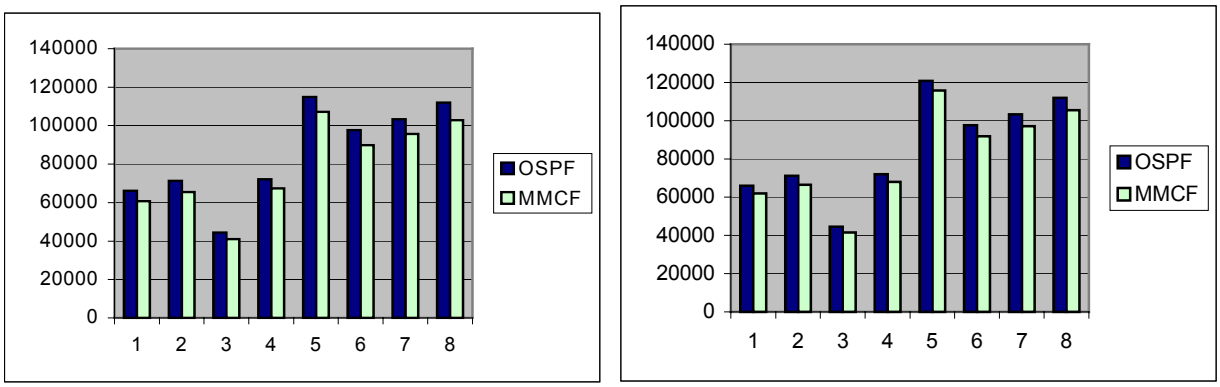


Figure 4. Numerical results for both BW and delay considerations a) Topology 1, b) Topology 2

Figure 4a shows the results for the MMCF and OSPF schemes for Topology 1. On average, MMCF saves 7.6% cost over OSPF (RFC2676). Figure 4b depicts the results for the MMCF and OSPF schemes for Topology 2. Once again, MMCF outperforms OSPF by reducing the cost by 5.85%

Figure 5 compares the results obtained for the two models for network Topology 1. The results show that in the case of OSPF, there is only one slight change in cost (Simulation 5) while in the case of the MMCF, the delay parameter affects the results obtained for all cases.

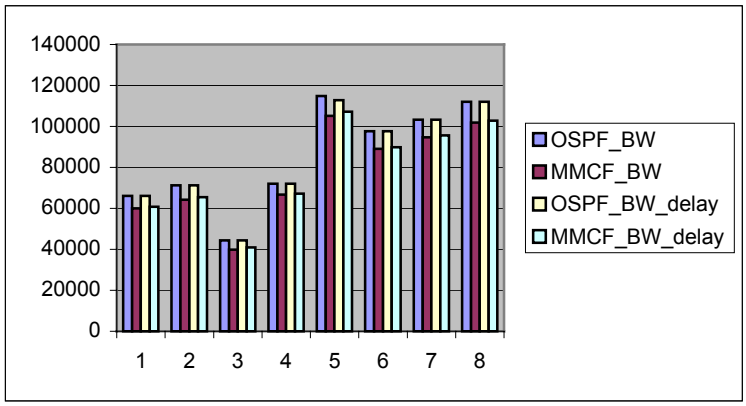


Figure 5. Comparison of Bandwidth vs. Bandwidth & delay schemes

5. CONCLUSIONS

The objective of our research has been to develop a cost-savings routing algorithm for supporting VPN services. A performance study was conducted for two versions of the proposed routing scheme 1) bandwidth reservation guarantees and 2) bandwidth and delay guarantees. From the analysis of our results the following general conclusions can be made.

Both OSPF and MMCF schemes are designed to meet the VPN users' requirements. However, the MMCF algorithm seems more attractive than OSPF in terms of cost-savings for a VPN service provider. Among the two topologies, MMCF obtains the best record - 10.2% cost-savings than OSPF in Topology 1.

The results also show that MMCF with the condition of bandwidth reservation is more effective than the scheme guaranteeing bandwidth and delay. The reason is that both OSPF and MMCF can meet the customer's requirements, but the design algorithms are different. OSPF focuses on determining the shortest hops and MMCF focus on the link cost instead. In other words, although both bandwidth and delay requirements are satisfied by OSPF and MMCF, OSPF respects delay best and MMCF regards link cost best. In terms of service provider's revenue, MMCF is a better option than OSPF.

There are other QoS requirements such as jitter and packet loss could be included as well. Therefore, more work shall be done in order to find a better solution for both VPN users and service providers.

REFERENCES

[1] H. Liang, O. Kabranov, D. Makrakis, L. Orozco-Barbosa "Minimal Cost Design of Virtual Private Networks", in Proc. IEEE CCECE'02. Winnipeg, May 2002, pp. 1610 –1615.

[2] R. Cohen, G. Kaempfer, "On the Cost of Virtual Private Networks", IEEE/ACM Transactions on Networking, Vol. 8, No. 6, pp. 775-784, December 2000.

[3] A. Verma, P. Venkataram, "Performance of Centralizad Bandwidth Reservation Protocol in AVPNs", Computer Communications Review, Vol. 27, No. 3, pp. 48-66, July 1997

[4] L. Haeryong, H. Jeongyeon, K. Byungryong, and J. Kyoungpyo, "End-to-end Architecture for VPNs: MPLS VPN Deployment in a Backbone Network", in Proceedings IEEE International Workshop on Parallel Processing, Toronto, August 2000, pp. 479-483.

[5] T. Braun, M. Guenter, and I. Khalil, "Management of Quality of Service Enabled VPNs", IEEE Communications Magazine, Vol. 39, No. 5, pp. 90-98, May 2001

[6] OSPF version 2, Ascend Communications, Inc. April 1998, RFC 2178.

[7] R. Ahuja, T. Magnani, B. Orlin, Network Flows, Theory, Algorithms and Applications, Prentice Hall, 1993.

[8] J. F. Kurose, K. W. Ross, Computer Networking: A top-Down Approach Featuring the Internet, Prentice Hall, 2001.

[9] WIDE project http://www.wide.ad.jp/