Configuration of Protected Virtual Private Networks

Markosz Maliosz, Tibor Cinkler
{Maliosz, Cinkler}@ttt-atm.bme.hu
Department of Telecommunications and Telematics
Budapest University of Technology and Economics
Pázmány Péter sétány 1/D, Budapest 1117, Hungary

Abstract

The route configuration of Virtual Private Networks (VPNs) over a given physical network is addressed considering the protection. We analyze protection at two different layers, first when the operator protects the virtual links of the VPN and second when the protection is done within the VPN. The problem is formulated as a general model without specializing to any particular network type, however the proposed methods can be used for various SDH, ATM, IP, MPLS and WR-DWDM Networks. The service demands of VPNs are characterized by the *bandwidth requirements* of node-pairs. Given the capacity matrix of the physical network and the traffic demand matrices of the VPNs, the protected VPN configuration is sought which minimizes the number of links used by the VPNs, and results in global optimum. Numerical results from calculations on sample networks show the properties of the protection at different layers.

Introduction

Virtual Private Networks have been increasingly wide-spread and used recently. More and more users require privacy and QoS guarantees over the public network infrastructure. Virtual Private Networks support the communication requirements of a closed group of users with special handling of privacy and security. The typical application of VPNs is remote access for joint project workers, or for a home user to access the company intranet. Privacy and security is handled by the upper communication layers, however the planning of the Virtual Private Networks over a physical network is a key question considering the operating costs. To ensure reliability the design must be prepared for failures. Therefore, the VPNs will have redundancy, a working and a protection path will be spanned between the node pairs. The route determination of the VPNs obeying link capacity constraints must be optimized considering the requirements for the protection.

VPNs share the link bandwidth and the node resources among each other but the idea has several advantages. We do not have to build our own physical private network, only configure VPNs that reduces costs. When a VPN is inactive other VPNs can use its physical resources, and even in contrast to physical links, the VPNs can be simply reconfigured. The secure data transfer among the VPNs is provided by encryption of the communication. VPNs can be applied to different network architectures, e.g. to ATM or IP or to Multi-Service Networks. A VPN-Diffserv solution is proposed in [1].

Our model deals with *static bandwidth demands* and *analyzes the protection methods*. In [2] there are also static demands considered, the paper plans to embed a VPN into a larger network while we place multiple VPNs at the same time into the network. In [3] dynamic relations are in scope with capacity resizing and stochastic fair sharing, but without protection. The resource allocation in conjunction with the routing design has been analyzed in [4,5,6] over multi-service networks with QoS constraints. Various tools are used like asymptotic approximations to reduce the complexity of the numerical calculations, multiplexing inside a VPN and introducing priorities between the traffic classes. Network dimensioning is addressed in [7] and the methodology is presented for determining the sizes of VPNs.

In our framework multiple VPNs exist over the same physical network. The data paths can be protected at link layer and at VPN layer. The *link layer protection* means that each traffic demand between node pairs belonging to a VPN will have two paths reserved, both of them within that VPN. These two paths should be either link disjoint, if we want to protect our services against link failures, or node disjoint, if we want protection against node failures as well. The *protection at VPN layer* means that the links that form the VPN (the virtual links) will be protected and not each traffic demand, i.e. there will be a working VPN skeleton and

a protection VPN skeleton. (see Fig. 1) The skeletons are formed form the virtual links. In this case, only the link independence can be interpreted, because we deal with the VPNs only, we do not know the actual paths of the traffic demands. There will be always common points for the working and protection VPNs, thus ensuring that in case of failure the traffic can be switched to the protection path. For clarifying the two different protection approaches: when a link goes down at the link layer protection each path in each VPN concerning that link will be rerouted. However, at the VPN layer each path in each VPN concerning that link will be rerouted, i.e. whole VPNs will be rerouted from the working skeleton to the protection skeleton.

Node disjoint paths between a node pair in link layer protection

Link disjoint paths between a node pair in link layer protection

Working and protection VPN skeletons in VPN layer protection

Figure 1 Different Protection Methods

The goal is to find optimal VPN configuration by minimizing the number of virtual links. By VPN configuration, we mean route selection and dimensioning for all VPNs simultaneously. The traffic and capacity matrices are given, these inputs are static values, like a snapshot from the actual network state. This method can be used in practice e.g. by a service provider to plan the VPNs with protection according to a weekly or monthly orders of companies.

The service layer properties of a VPN are determined by the bandwidth requirement between each pair of nodes. For constant bitrate flows the bandwidth requirement is the exact value, however, if the traffic is bursty the effective bandwidth approximation can be used here.

The calculated routes can be applied in practice using constraint-based routing instead of destination-based, for example in an MPLS VPN architecture [8,9].

The models

MinVL at Link Layer

Link Disjoint Case

This method minimizes the VPN cost, i.e. it minimizes the number of virtual links. *MinVL* is the abbreviation of Minimal Virtual Links. Let us assume the network is an undirected graph *U(N,L,C)*. *N* is the set of nodes, *L* is the set of links between the nodes, and *C* is the capacity matrix, which contains the capacities of the physical links. The traffic matrices are given for each VPN, they contain the bandwidth demand for each node pair in the VPN. The variables in the optimization are:

$X1_l^d$ and $X2_l^d$ are binary variables, where *l* is a physical link and *d* is a demand between two nodes

$X1_l^d \in \{0,1\}$ $X2_l^d \in \{0,1\}$

Y_l^p is binary variable, where *l* is a physical link and *p* is the ordinal number of a VPN

$Y_l^d \in \{0,1\}$

$X1_l^d$ and $X2_l^d$ represent, whether link *l* carries traffic, which belongs to demand *d*. $X1_l^d$ is for the working and $X2_l^d$ is for the protection path. Y_l^p represents, whether link *l* is used by VPN *p* or not. When the variables are "0" then there is no traffic on link *l*, value of "1" indicates that there is traffic on that link. *l* is *(i,j)* pair of numbers, where *i* and *j* are the ordinal numbers of nodes, namely link *l* is between nodes *i* and *j*. *d* is an *(i,j,b,v)* tuple, *i,j* is a pair of numbers, where *i* and *j* are the ordinal numbers of nodes, *b* is the bandwidth requirement of the demand, *v* is the ordinal number of the VPN, and it means that there is a demand between nodes *i* and *j* with bandwidth *b* in VPN *v*.

In case of l only those *(i,j)* pairs of numbers are valid where *(i,j)* element is non-zero in the capacity matrix, these *(i,j)* pairs form the set L ($l \in L$). In case of d, when the bandwidth requirement (b) between *(i,j)* is not zero, then it is a valid demand. These form the set D ($d \in D$).

$$l = \{(i, j) \mid (i, j) \in L, L \subset N^2\}$$

$X1_l^d$, $X2_l^d$ and Y_l^p variables cover the same quantity, but in different ways, namely the used links in different approaches. While $X1_l^d$ and $X2_l^d$ show the link usage according to the demands between node pairs, Y_l^p shows whether a link is used by a particular VPN or not.

The cost of the VPNs is defined as follows:

$$C_{VPN} = \sum_{\forall p} \sum_{l \in L} Y_l^p \qquad (1)$$

The objective functions is:

$$\min(C_{VPN})$$

The constraints:
Flow conservation constraints:

$$\sum_{\forall (i,j) \in L} X1_{(i,j)}^d - \sum_{\forall (j,k) \in L} X1_{(j,k)}^d = \begin{cases} -1, & \text{if } j \text{ is source of } d \\ 1, & \text{if } j \text{ is destination of } d \\ 0, & \text{otherwise} \end{cases} \quad \forall j \in N, \forall d \in D \qquad (2)$$

$$\sum_{\forall (i,j) \in L} X2_{(i,j)}^d - \sum_{\forall (j,k) \in L} X2_{(j,k)}^d = \begin{cases} -1, & \text{if } j \text{ is source of } d \\ 1, & \text{if } j \text{ is destination of } d \\ 0, & \text{otherwise} \end{cases} \quad \forall j \in N, \forall d \in D \qquad (3)$$

These equations ensure that only sources originate and destinations sink the traffic flow. At the intermediate nodes the incoming and outgoing traffic is equal. This is expressed for both working and protection paths. The first sum stands for the traffic coming in into node j and the second sum is the outgoing traffic.

Capacity constraint

$$\sum_{\forall d \in D} (X1_l^d + X2_l^d) b^d \le B_l \qquad \forall l \in L \qquad (4)$$

B_l stands for the physical capacity of link l, b^d is the bandwidth requiremnt of demand d. $X1_l^d$, $X2_l^d$ indicate whether the working or protection path is using link l. This constraint expresses that the total capacity partitioned among the VPNs should not exceed the physical capacity bound.

Diversity constraint

$$X1_l^d + X2_l^d \le Y_l^p \qquad \forall l \in L, \forall p, \forall d \in D^p \qquad (5)$$

D^p is the set for those demands, that belong to VPN *p*. $Y_l^p \in \{0,1\}$ therefore at most only one, $X1_l^d$ or $X2_l^d$ can be "1" providing link independence.

Node Disjoint Case

This model adds only one more constraint to the previous case. Namely, the two paths must not have common nodes.

Diversity constraint II

$$\sum_{l(i,j)\in L,\, i \text{ is not source of } d,\, j \text{ is not destination of } d} (X1_l^d + X2_l^d) \le 1 \qquad \forall d \in D \qquad (6)$$

This constraint expresses that there cannot be two paths going through node *i*, unless *i* is the *source* or *destination* of the demand.

MinVL at VPN Layer

As mentioned in the Introduction at VPN layer only the link disjoint case can be interpreted. This method minimizes the VPN cost, i.e. it minimizes the number of virtual links while considering that the whole VPN must be protected.

The variables in the optimization are:

$X1_l^d$ and $X2_l^d$ are binary variables, where *l* is a physical link and *d* is a demand between two nodes

$X1_l^d \in \{0,1\}$ $\qquad$ $X2_l^d \in \{0,1\}$

$Y1_l^p$ and $Y2_l^p$ are binary variables, where *l* is a physical link and *p* is the ordinal number of a VPN

$Y1_l^d \in \{0,1\}$ $\qquad$ $Y2_l^d \in \{0,1\}$

$X1_l^d$ and $X2_l^d$ represent whether link *l* carries traffic which belongs to demand *d*. $X1_l^d$ is for the working and $X2_l^d$ is for the protection path. $Y1_l^p$ and $Y2_l^p$ represent whether link *l* is used by the working or protection VPN *p*. When the variables are "0" then there is no traffic on link *l*, while value "1" indicates that there *is* traffic on that link. *l* and *d* are the same demands as above.

$X1_l^d$, $X2_l^d$, $Y1_l^p$, $Y2_l^p$ variables cover also the same as at the Link Disjoint Case, namely the used links in different approaches. While $X1_l^d$ and $X2_l^d$ show the link usage according to the end-to-end demands, $Y1_l^p$ and $Y2_l^p$ shows whether a link is used by the working or protection VPN.

The cost of the VPNs is defined as follows:

$$C_{VPN} = \sum_{\forall p} \sum_{l \in L} (Y1_l^p + Y2_l^p) \qquad (7)$$

The objective functions is:

$$\min(C_{VPN})$$

The constraints are partly from the Link Layer Model, therefore equations (2), (3) and (4) are applied here as well.

Additional capacity constraints:

$$X1_l^d \le Y1_l^p \qquad \forall l \in L, \forall p, \forall d \in D^p \qquad (8)$$

$$X2_l^d \le Y2_l^p \qquad \forall l \in L, \forall p, \forall d \in D^p \qquad (9)$$

D^p is the set for those demands, that belong to VPN *p*. If $X1_l^d$, $X2_l^d$ is "1" (showing link *l* is used for carrying the traffic for demand *d*), it involves that $Y1_l^p$, $Y2_l^p$ should be "1" indicating that link *l* is used by VPN *p*.

The diversity constraint in this model is:

$$Y1_l^p + Y2_l^p \le 1 \qquad \forall l \in L, \forall p \qquad (10)$$

To ensure the link disjoint property, the following constraint must be added too, otherwise it could happen that the protection path were use the same link in the opposite direction.

$$Y1_{(i,j)}^p = Y2_{(j,i)}^p \qquad \forall (i, j) \in L, \forall p \qquad (11)$$

Optimization Process

Network topologies

We tested the models on sample network topologies with traffic demands for different scenarios. Four different topologies were investigated a 6-node network with 7 links, a 9-node network with 12 links, a 15-node network with 25 links and a 25-node network with 50 links (Fig. 2). Different traffic demands were selected for the VPNs in each case.

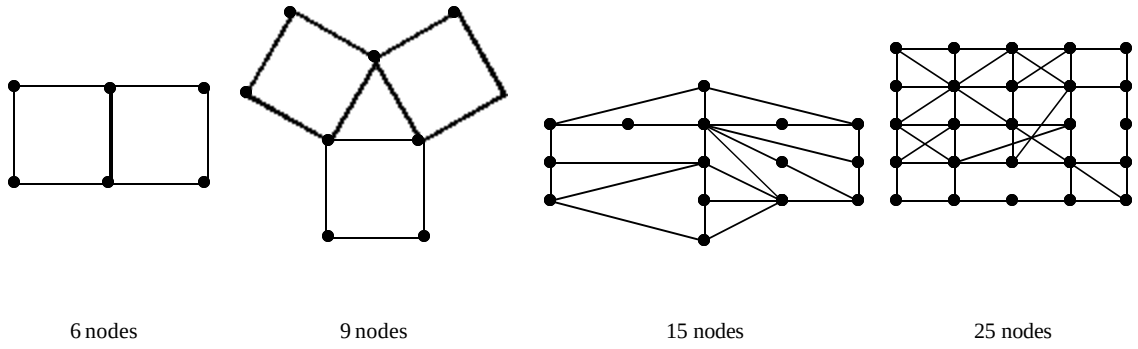

Figure 2 Network Topologies

Results

ILOG CPLEX optimizer [10] was used to solve the MIP problems. The route configuration results are compared to the results of a model without protection [11]. The results without protection are the trivial solutions in this case, since the link capacities are large enough to accommodate the protection paths as well. The charts in Fig. 3 show the number of hops, Fig. 4 shows the total capacity used in each case. Out of the $X1_l^d$, $X2_l^d$ results the smaller values are assigned to the working paths and the others to the protection paths. The number of hops and the capacity usage are summarized separately by working and protection paths. Bar 1 is the configuration *without protection*, bar 2 is the *link disjoint link layer protection*, bar 3 is the *node disjoint link layer protection*, and bar 4 is the *VPN layer protection*. As you can see, from the 15-node network there is no bar 4, because the MIP solver tool calculated hours long without results, which are not really in the acceptable time limit. Table 1 shows the number of virtual links, i.e. the result of the objective function, and the time consumption of the solver processes. The time consumption of not protected networks is only several hundredths of seconds, except the 25-node network, which has many links, causing higher complexity. Comparing the node disjoint and link disjoint cases, the node disjoint method can be solved quicker, although it has more constraints. The VPN layer protection lasts obviously longer than the others, since it is a more complicated problem.

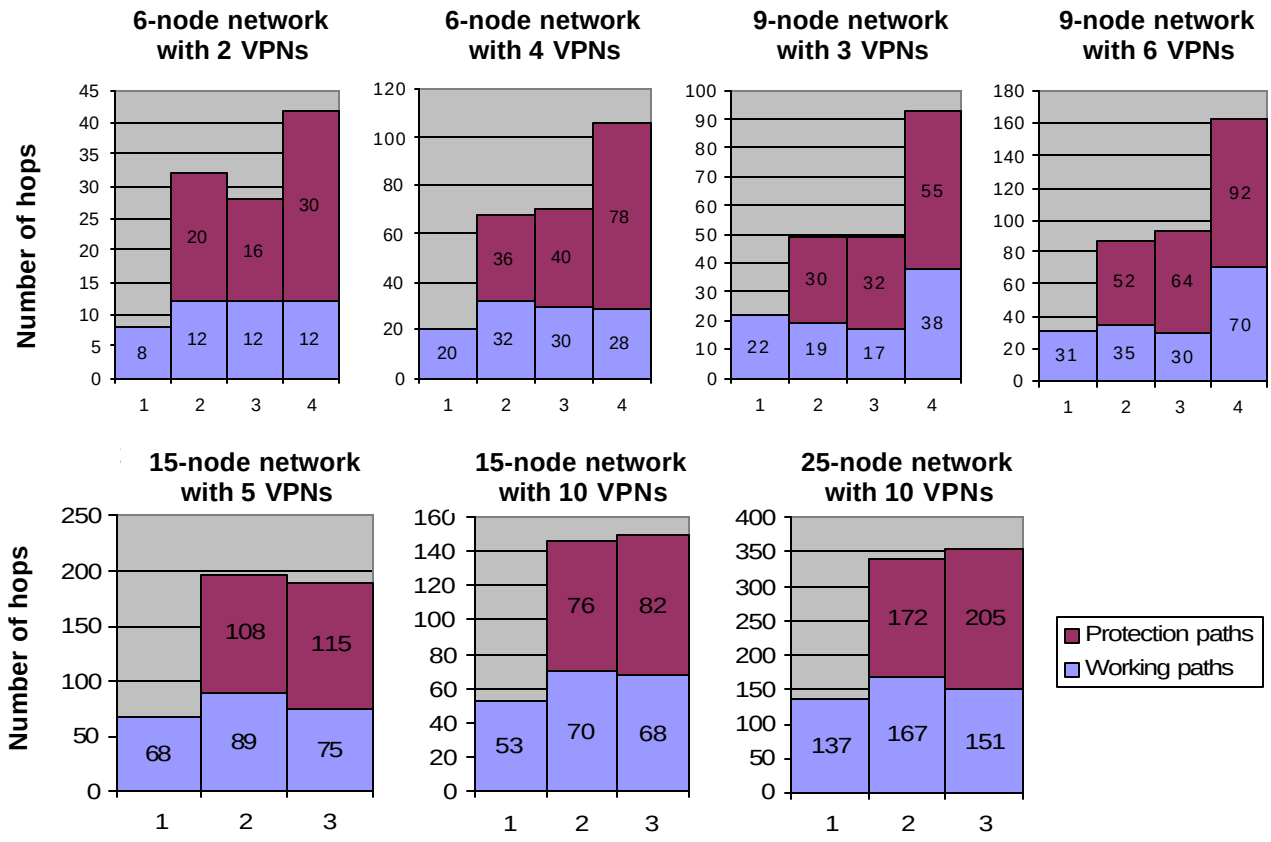

Figure 3 **Number of hops for 4 different networks**

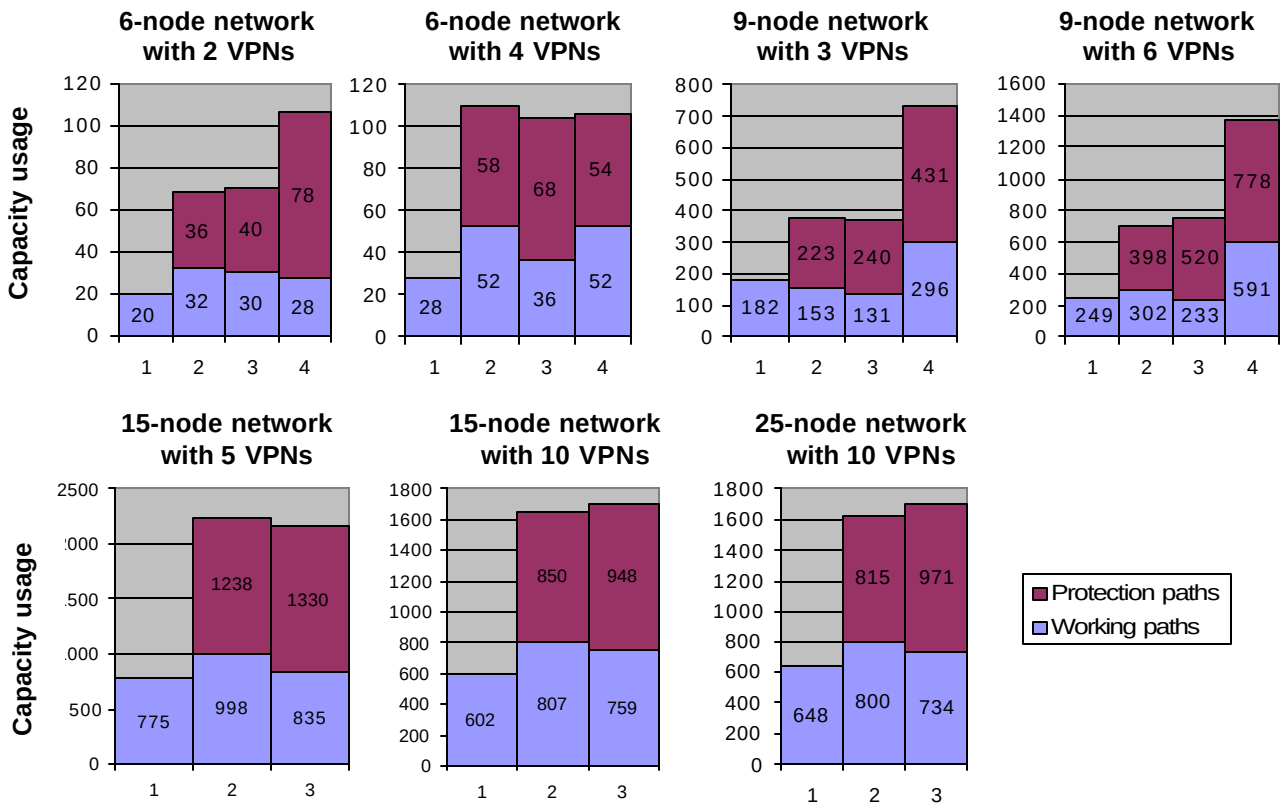

Figure 4 **Capacity usage for 4 different networks**

The number of virtual links (which is the objective function of the optimization) are increasing, at least doubled, when we use protection at the link layer, and even four or five times more in case of VPN layer protection. However, the number of virtual links in case of small network nodes is the same when we compare the link disjoint and node disjoint link layer protections. They have fewer links, therefore the two solutions could not really differ from each other.

Fig. 3 shows that the VPN layer protection requires more hops, i.e. longer paths. The link disjoint and node disjoint link layer protection are almost at the same level in this aspect. In large networks with large number of VPNs the node disjoint solution requires slightly more hops. In Fig. 4 the results are similar to Fig. 3, namely longer paths result in higher capacity usage. The same tendency can be observed as in Fig 3, the link layer protection requires approximately doubled capacity, and VPN protection requires the doubled capacity of the link layer protection.

	Without protection		Link disjoint link protection		Node disjoint link protection		VPN protection	
Network nodes / VPNs	Solution time (sec)	Number of Virtual Links	Solution time (sec)	Number of Virtual Links	Solution time (sec)	Number of Virtual Links	Solution time (sec)	Number of Virtual Links
6 / 2	0.01	4	0.02	16	0.02	16	0.4	28
6 / 4	0.02	9	0.23	31	0.15	31	1.35	56
9 / 3	0.03	13	0.06	28	0.07	28	7.34	56
9 / 6	0.05	22	0.1	53	0.12	53	448.8	102
15 / 5	0.58	41	7.62	95	1.88	98		
15 / 10	0.13	49	1.59	124	1.41	130		
25 / 10	69.09	72	339	173	11.42	175		

Table 1 Solution times and number of Virtual Links

You can observe that there are items, where the working part of the protected network has fewer hops or uses less capacity than the unprotected network. The reason is that the optimization minimizes the number of virtual links, which are the same in these cases (see Table 1), and not the number of hops. The average of the working and protection values in number of hops or capacity usage are still greater than in the unprotected case. The node disjoint cases have the largest differences between the working and protection values.

To show the differences between our approach – to minimize the number of Virtual Links – and the usual one, where the total cost (in this case the capacity usage) is minimized we present an example in Table 2. Three different objectives were aimed in the 9-node network 6 VPNs configuration. The first case, where only the capacity usage is minimized equals to the case when the VPNs are not considered, i.e. each demand is independently routed in the network. The second deals only with minimizing the number of Virtual Links, and the third one is a combination of the formers. The results show that minimizing only the capacity usage yields larger numbers in Virtual Links. Minimizing only the number of Virtual Links obviously yields higher capacity usage and utilizes more hops. The combined solution is near to the second solution regarding the number of Virtual Links. It provides smaller capacity usage than the second, but it is still higher than the first solution.

	Minimizing	Number of Virtual Links	Number of hops			Capacity usage		
			Working	Protection	Sum	Working	Protection	Sum
Without protection	the capacity usage	24	29		29	226		226
	the number of virtual links	22	31		31	249		249
	the sum of capacity usage and number of virtual links	24	29		29	226		226
Link disjoint link layer protection	the capacity usage	67	29	50	79	238	395	633
	the number of virtual links	53	35	52	87	302	398	700
	the sum of capacity usage and number of virtual links	54	32	48	80	266	370	636
Node disjoint link layer protection	the capacity usage	65	29	50	79	238	395	633
	the number of virtual links	53	30	64	94	233	520	753
	the sum of capacity usage and number of virtual links	54	30	50	80	248	388	636
VPN layer protection	the capacity usage	108	39	41	80	313	332	645
	the number of virtual links	102	55	70	125	458	546	1004
	the sum of capacity usage and number of virtual links	102	38	45	83	301	365	666

Table 2 Different objective functions on 9-node network with 6 VPNs

Fig. 5 illustrates the path length distribution in two configurations. The link layer protection methods attempt to concentrate the traffic on shorter paths, while the VPN layer protection has another preferences. It does not deal with each path one-by-one, but with the VPN as a whole, therefore the path length distribution shows that this solution has more longer paths.

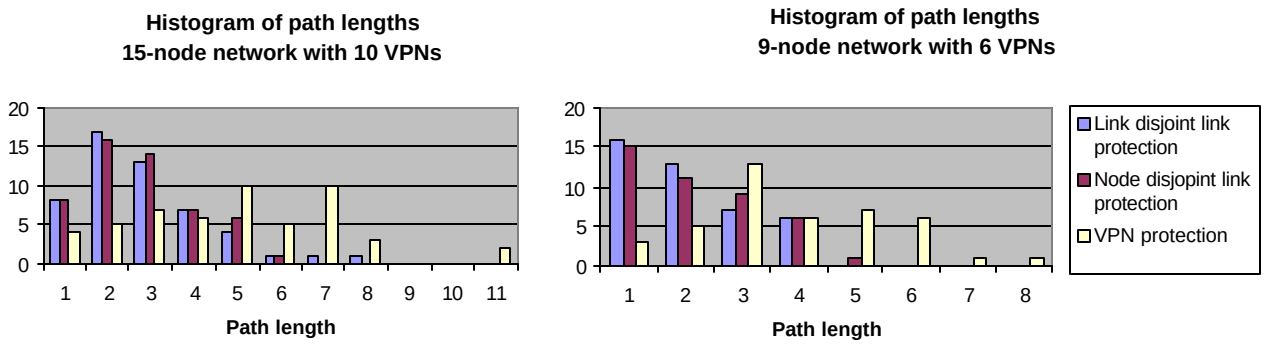

Figure 5 Path length distribution

Conclusions

Joint route selection and resource allocation of VPNs with different protection methods is discussed. Different methods were described to get the optimal VPN working and protection configuration over the physical network. The goal is to use minimal number of links, but with protected paths. The solutions were compared to each other, and to the unprotected case. The methods try to concentrate the traffic on fewer links, which results higher capacity usage, but this way the VPNs will have smaller expansion, i.e. they use less virtual links. Large networks require larger computational capacity, therefore the solution process should be enhanced with heuristics. The VPN layer protection is more complicated problem, than the link layer protection, however ensures the protection of whole VPNs' virtual links. It requires about twice as much capacity than the link layer protection, which requires about twice as much than the unprotected configuration. The link or node disjoint link layer protection gives the opportunity to have different levels of protections in the system. Based on such results service providers can choose among the protection methods according to their preferences.

References

[1] Ibrahim Khalil, Torsten Braun, Edge Provisioning and Fairness in VPN-Diffserv Networks, The 9th International Conference on Computer Communication and Network (ICCCN 2000), October 16-18, 2000, Las Vegas, USA.

[2] Martin Oellrich, Minimum-Cost Disjoint Virtual Private Networks under Edge Dependences, Boca 2000 – Fifth INFORMS Telecommunications Conference, March 5-8, 2000, Boca Raton, Florida

[3] Rahul Garg, Huzur Saran, Fair Bandwidth Sharing Among Virtual Networks: A Capacity Resizing Approach, INFOCOM 2000, Tel-Aviv

[4] D. Mitra and K. G. Ramakrishnan, A Case Study of Multiservice, Multipriority Traffic Engineering Design for Data Networks, Proc. IEEE GLOBECOM 99, pp.1077-1083, Dec.1999

[5] D. Mitra, J. A. Morrison and K. G. Ramakrishnan, Optimization and Design of Network Routing using Refined Asymptotic Approximations, Performance Evaluation, vol. 36-37, pp.267-288, 1999

[6] D. Mitra, J.A. Morrison and K. G. Ramakrishnan, Virtual Private Networks: Joint Resource Allocation and Routing Design, Proc. IEEE INFOCOM 99

[7] N. Anerousis, "Dynamic Virtual Private Network Dimensioning in Cost-Sensitive Environments", IEEE Globecom, Rio de Janeiro, Brazil, December 1999.

[8] B. Davie, Y. Rekhter, MPLS – Technology and Applications, Academic Press, 2000

[9] I. Pepelnjak, J. Guichard, MPLS and VPN Architectures, Cisco Press

[10] ILOG CPLEX 6.5 Documentation

[11] M. Maliosz, T. Cinkler, Optimizing Configuration of Virtual Private Networks, Polish-Czech-Hungarian Workshop on Circuit Theory, Signal Processing, and Telecommunication Networks, Budapest, Hungary, 14-17 September 2001