2005

Traffic engineering and path protection in MPLS virtual private networks

Pooja S. Aniker
Louisiana State University and Agricultural and Mechanical College

TRAFFIC ENGINEERING AND PATH PROTECTION IN MPLS VIRTUAL PRIVATE NETWORKS

A Thesis

Submitted to the Graduate Faculty of
the Louisiana State University and
Agricultural and Mechanical College
in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

in

The Department of Electrical and Computer Engineering

by
Pooja S Aniker
B.E., Bangalore University, India, 2001
May 2005

Acknowledgments

I would like to extend my sincere gratitude to my advisor Dr. Morteza Naraghi-Pour for his excellent guidance and support without which this work would not be possible. I am very thankful to him for helping me to understand the concepts and organize my ideas. Throughout the process of working on my thesis, he has been very patient, understanding and supportive. I am very grateful for all the help that he has provided me.

I also like to thank Dr.Subhash Kak and Dr. Ramanujam for being a very supportive and understanding committee.

I am thankful to my parents and family for instilling confidence and encouraging me throughout my Master's Degree. Their blessings, love and well wishes have always been with me.

Last, but not the least I sincerely thank all my friends for their support and patience. I could not have accomplished this without their help.

Table of Contents

List of Tables

List of Figures

Abstract

Traffic Engineering (TE) attempts to establish paths for the flow of data in a network so as to optimize the resource utilization and maximize the network performance. One of the main goals of Traffic Engineering is to bring about efficient and reliable network operations. Constraint based routing is the key to Multiprotocol label switching TE. Constraint based routing helps to manage traffic paths within a MPLS network and allows for traffic to flow along certain desired paths. MPLS also supports explicit routing thus providing TE capabilities. MPLS TE enables resiliency and reliability to be built into networks, thus increasing the value and availability of the network. TE is deployed in MPLS networks by providing TE extensions to interior gateway protocols like OSPF and IS-IS. MPLS creates a connection oriented model over the traditional connectionless framework of IP based networks. This connection oriented model helps to overcome several shortcomings of the IP network and also provide the necessary framework to give quality guarantees to IP traffic. Quality of Service (QoS) can be built into MPLS networks where TE is used. MPLS has made significant progress in recent years and is used for deployment of networks all over the world. In this thesis, we propose several constraint-based routing algorithms for MPLS based VPN's. Our algorithms support routing of both Quality of Service (QoS) and BE traffic over the MPLS network. We have implemented a route based and a link based approach for routing of QoS and BE traffic. We also implement the $1 + 1$ and $1 : 1$ link disjoint and node disjoint path protection mechanisms for the QoS traffic. We study the effect of the various parameters used in our equations such as epsilon, granularity, earning rate and hop count. The problem is formulated as a multicommodity flow (MCF) problem and is solved using the optimization tool - ILOG CPLEX. Our approach is scalable to large networks having a number of VPN's.

Chapter 1

Introduction

In this chapter we provide an overview of the working of MPLS in Section 1.1. The concept of Virtual Private Networks (VPN's) and an overview of the architecture and operation in MPLS VPN's is discussed in Section 1.2. In Section 1.3 we explain the concepts of Traffic Engineering and Constraint Based Routing. Path Protection is introduced in Section 1.4.

1.1 Multiprotocol Label Switching

In a traditional IP network the router analyzes the destination address in the packet header at each hop and makes a independent forwarding decision as the packet travels from the source to the destination. IP forwarding is based on routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP). These protocols are designed to find the shortest path from the source to the destination and do not consider factors such as latency and traffic congestion. In order to overcome some of these restrictions Multiprotocol Label Switching (MPLS) was introduced. MPLS establishes a connection oriented network overlaid onto the connectionless framework of IP networks. Due to this connection oriented architecture, a number of new techniques for traffic management are available. In MPLS packets are forwarded by label swapping or label switching. The labels are contained in a MPLS header inserted into the data packet. The label is a short fixed length physically contiguous identifier that tells the routers how to forward the packets from the source to the destination. The packets follow a predetermined path called the Label Switched Path (LSP). LSP is also referred to as a MPLS tunnel. It is simply a concatenation of one or more hops in the network. Signaling protocols such as Resource reSerVation protocol with Tunneling Extensions (RSVP-TE) and Label Distribution Protocol (LDP) can be used to establish connections and distribute labels. These protocols establish paths through the MPLS network and reserve network resources along the path according to the requirement. The routers in the MPLS network are called the Label Switch Routers (LSR's) and the routers in the edge of the network are called Label Edge Routers (LER's). The router at the entry point of the tunnel is referred to as the ingress router and the router at the end point is called the egress router. When packets enter the network they are classified into Forwarding Equivalence Classes (FEC). All the packets belonging to the same FEC

receive the same forwarding treatment. A FEC is a logical entity created by the router to represent a class of packets. After the initial classification the packets are then assigned a label and the path corresponding to that FEC by the LER. The label is used to identify a FEC. The packets are then forwarded along the LSP. At each hop, the LSR removes the incoming label and attaches a outgoing label. This outgoing label tells the next router how the packet should be forwarded. Fig 1.1 shows a typical MPLS network and the associated elements. The central cloud represents the MPLS network. The customer edge routers (CE routers) interface with the provider edge routers (PE routers). The PE router at the ingress point attaches the MPLS label to the packet and the PE router at the egress point removes the MPLS label from the packet. The CE and PE routers are the LER's. Within the MPLS domain, the Provider (P) routers forward the traffic hop by hop based on the labels. The P routers are the LSR's.

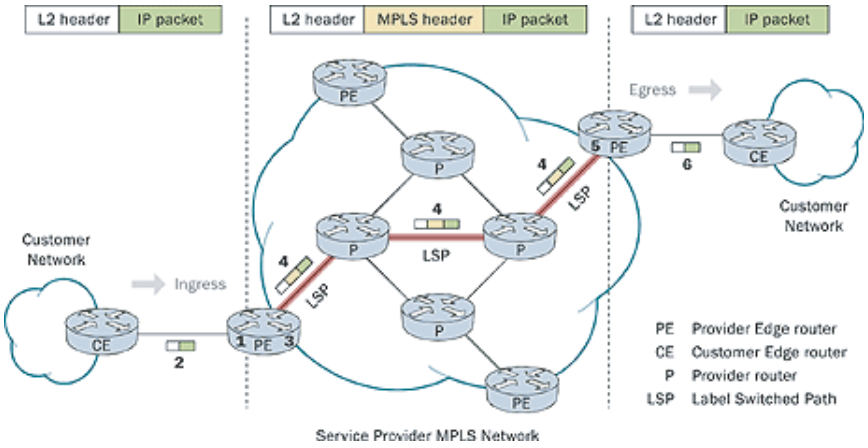

Figure 1.1: MPLS Network

As the name suggests, the techniques of MPLS are applicable to any network layer protocol. MPLS is a framework of functions. MPLS combines the benefits of packet forwarding based on Layer2 Switching with that of Layer3 Routing. MPLS also provides the benefit of Traffic Engineering (TE). It can also be used to set up Virtual Private Networks.

1.2 Virtual Private Networks

A Virtual Private Network is a private communication network that makes use of the public telecommunication infrastructure to transmit data. It can be used within a single organization or several different organizations. It uses tunneling protocols to maintain confidentiality of data and message integrity. The main purpose of a VPN is to provide a company with the capabilities of private leased lines at a much lower price by using the shared public infrastructure. The Internet is a shared public infrastructure with open

transmission protocols. Hence, in order to set up a VPN, it must include packet encapsulation or tunneling, encryption and sender authentication in order that the data reaches the destination without being tampered.

- **MPLS VPN Architecture Overview**

Since MPLS allows the tunneling of packets from the ingress router to the egress router VPN applications that require this capability can be easily built. VPN's built on MPLS provide users with all the benefits of MPLS such as traffic engineering, Quality of Service (QoS) and separation of traffic. MPLS VPN's allow service providers to deploy scalable VPN's and provide value added services. MPLS VPN's can be divided into two categories. One is the customer based VPN where the VPN is configured on the customer side equipment. The second category is the network based VPN where the VPN is configured on the service provider equipment and is operated by the provider. MPLS VPN's are network based and offer considerable cost savings and increased scalability. MPLS provides for traffic separation by uniquely identifying each VPN flow and setting up circuit like connections. A VPN consists of CE routers attached to the customer site. The customer sites use the CE routers to communicate with other customer sites. Only the PE routers are aware of the VPN's. The MPLS architecture is as shown in 1.2. The figure shows five customer sites communicating with three VPN's.

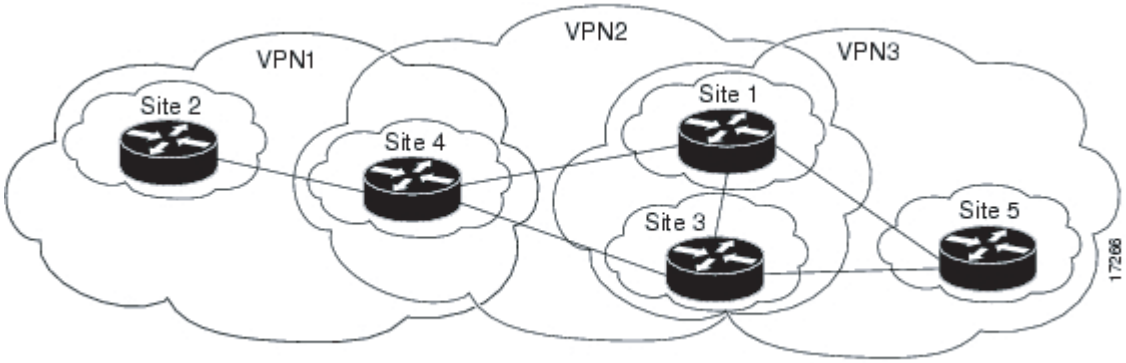

Figure 1.2: MPLS VPN Architecture

- **MPLS VPN Operation Overview**

Fig 1.3 shows the operation of a MPLS VPN. The CE router provides the PE router with the routing information of the corresponding customer site. This routing information is stored in a distinct routing and forwarding table called the Virtual Routing and Forwarding table (VRF) in the PE router to guarantee isolation between the various VPN's. Thus the PE router maintains a separate VRF table for each VPN. Each PE router needs a unique router ID that is used to allocate a label and enable VPN forwarding in the backbone of

the network. Each PE router allocates a unique label to each route in each VRF. The PE routers exchange information about the VPN customers and routes among themselves by using Border Gateway Protocol (BGP) as the routing protocol. In order to make the IP addresses used within a VPN unique, they are concatenated with a 64 bit prefix called a route distinguisher (RD). In order to uniquely recognize the VPN originated IP packets each of the packets are labeled by the ingress PE router with a label that uniquely identifies the egress PE router.

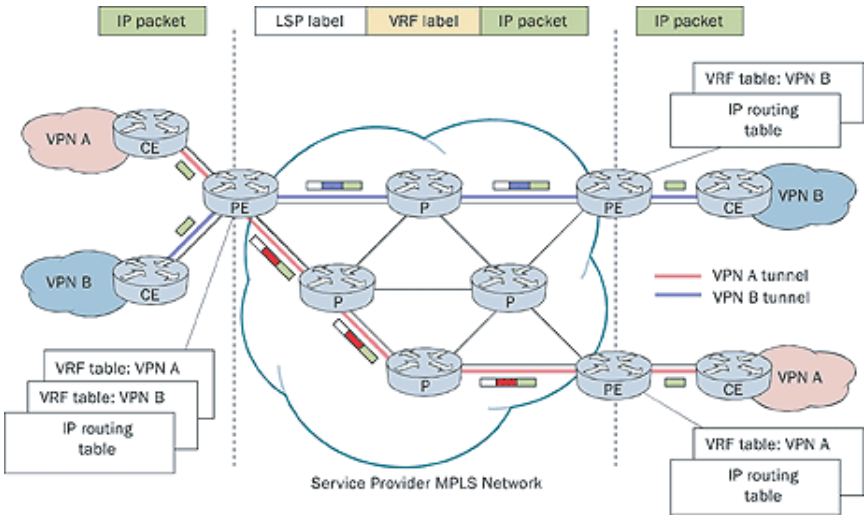

Figure 1.3: MPLS VPN Operation

Each PE-router assigns a unique label for each route in each VPN routing and forwarding (VRF) instance. These labels are then propagated along with the corresponding routes to all the other PE-routers . The PE-routers then install the received routes and the label assigned by the egress routers in the VRF tables. The MPLS/VPN network is now ready to forward VPN packets. When a VPN packet is received by the ingress PE-router, the corresponding VRF is examined, and the label associated with the destination address by the egress PE-router is obtained. Another label, pointing toward the egress PE-router, is obtained from the global forwarding table. Both labels are combined into an MPLS label stack, are attached in front of the VPN packet, and are sent toward the egress PE-router. All the P-routers in the network switch the VPN packet based only on the top label in the stack, which points toward the egress PE-router. Because of the normal MPLS forwarding rules, the P-routers never look beyond the first label and are thus completely unaware of the second label or the VPN packet carried across the network. The egress PE-router on receiving the labeled packet, drops the first label, and performs a lookup on the second label, which uniquely identifies the target VRF. A lookup is performed in the target VRF, and the packet is sent toward the proper CE-router.

1.3 Traffic Engineering

Traffic Engineering (TE) is the process of selecting suitable paths for the flow of data in a network so as to efficiently utilize the network resources and enhance the network performance while maximizing the network revenue. One of the main goals of Traffic Engineering is to bring about efficient and reliable network operations. Traffic Engineering attempts to compute a path from the source node to the destination while adhering to constraints such as bandwidth,delay and other administrative requirements. After the path is computed, Traffic Engineering enables the establishment of the path and also maintains the forwarding capability of the path. In IP routing traffic between two points is sent over the shortest path available even though multiple paths may exist. During traffic congestion, this may lead to a few routes being overused and some routes being underused. This leads to inefficient utilization of network resources. MPLS manages bandwidth more efficiently by specifying explicit routes and by setting certain bandwidth guarantees. MPLS has a number of techniques that support Traffic Engineering. MPLS computes a path at the source taking into account all the constraints. This is possible only if the source has some way of gathering the network information either locally or from other routers. In addition to supporting explicit routing, MPLS also has the ability to distribute information about network resources and topology, reserve network resources and modify link attributes. MPLS Traffic Engineering (MPLS TE) increases the availability and the value of the network to users. TE is built into MPLS networks via traffic engineering extensions to protocols such as OSPF and IS-IS. OSPF-TE and IS-IS-TE carry additional information such as link bandwidth, link utilization, delay, priority, etc. to allow the network to utilize paths that meet service requirements, resource availability and other constraints. RSVP-TE is commonly used for MPLS Traffic Engineering. MPLS TE is deployed in the core of the MPLS network and it helps to reduce traffic congestion and enables efficient utilization of the available resources.

MPLS also supports Quality Of Service (QoS). QoS is defined in **RFC2386** as 'a set of service requirements to be met by the network while transporting a flow.' A flow refers to a packet of data being transmitted with a certain level of QoS. QoS is basically a certain level of service provided to customers. Some of the characteristics that determine the level of service are probability of packet loss, bandwidth requirements, delay etc. QoS based routing is a mechanism wherein paths are determined on the basis of availability of network resources and QoS requirement. QoS routing selects routes that satisfy the QoS requirement. MPLS along with Differentiated Services (Diffserv) makes QoS support possible. Some of the techniques used by MPLS to provide QoS are IP Precedence, Random Early Detection (RED), Weighted RED, Weighted Fair Queuing (WFQ), Class -Based WFQ and Priority Queuing. Unlike MPLS TE, QoS is used at the edge of the MPLS network. It ensures that high priority packets get a preference over low priority traffic. Together, QoS and traffic engineering enable organizations to move away from multiple, specialized networks for voice, video, and data to a single converged IP/MPLS network, dramatically reducing overhead and cost.

Constraint Based Routing (CBR) is a mechanism of determining a path from the

source to the destination subjected to certain constraints such as link capacity, available bandwidth, delay requirement and administrative policies. It uses information about network resources, topology and traffic patterns to compute routes. CBR only determines the path and does not reserve any resources on the path. For reserving resources a reservation protocol such as RSVP has to be used. CBR manages traffic paths within a MPLS network, allowing the traffic to flow along desired paths. CBR can be online or offline depending on where the path computation is performed. Online CBR takes into account resource constraints and calculates one LSP at a time. Path calculation is performed at the routers and hosts without knowledge of new requested traffic. Online CBR can adapt to network changes and state updates. In Offline CBR, path computation is performed outside the network for a fixed traffic demand and network topology. Offline CBR helps to optimize network resource usage but it cannot adapt to network changes.

1.4 MPLS Path Protection

Since MPLS supports Traffic Engineering, it allows explicit routing of packets. This feature allows MPLS networks to pre-establish backup paths for the primary paths. Each of these backup LSP's have the same amount of bandwidth as the primary LSP's. Path Protection provides an end to end failure recovery mechanism for MPLS Traffic Engineering tunnels.The backup paths have the same source-destination pair as the corresponding primary paths. One or more LSP's are established in advance to provide failure protection for the protected LSP. If the primary LSP fails, the traffic is immediately temporarily switched onto the backup LSP's. It is important that the backup LSP's are either link disjoint or node disjoint with the primary LSP's i.e the backup LSP's do not share a link or a node with the primary LSP's else the failure of a shared link or node would affect both the primary and backup paths.

Rerouting is another technique of providing path protection. In this method, upon failure of the primary path the traffic is simply rerouted along a new path or path segment. No resources are reserved in advance until the fault occurs. This mechanism provides a higher resource utilization, but is slow compared to protection switching as the secondary path is established upon detection of a failure.

- **1+1 Path Protection mechanism**

In 1+1 path protection the backup path carries a copy of the traffic on the primary path. Upon detection of a failure, the traffic is routed along the backup path. The backup path resources are not available to low priority traffic. There is no sharing of the resources of the backup path. It is the fastest path protection mechanism. 1+1 path protection can be link disjoint or node disjoint.

- **1:1 Path Protection mechanism**

In 1:1 path protection, the resources of the backup path are available to low priority traffic. There is a sharing of the backup path resources. Upon detection of a failure, the low priority traffic is preempted and the traffic is switched from the primary to the backup LSP. 1:1 path protection can be link disjoint or node disjoint.

Chapter 2

Traffic Engineering for MPLS VPN's

2.1 Introduction

In section 2.2 we review off-line constraint-based algorithms for routing both Quality of Service (QoS) and Best Effort(BE) service classes. We review the notations used in the formulation of the multi commodity flow (MCF) problems and also discuss certain MPLS attributes such as label constraint and hop constraint.Our approach towards traffic engineering including link based and route based routing is introduced in 2.3. The experimental results showing the effects of various parameters on routing for several example networks is explained in 2.4.

2.2 Previous Work

In [1], Mitra and Ramakrishnan proposed a technique for multiservice, multipriority traffic engineering in QoS supported data networks using a multi-commodity flow problem. In their approach the high priority QoS traffic is routed first utilizing all the available link capacities. The Best Effort traffic is routed after QoS and is allowed to utilize the residual capacities. But this method had some drawbacks. In [4], Chung-Yu Wei proposed a method to overcome these drawbacks and extended the multi-commodity flow problem to support QoS and Best Effort routing in MPLS networks. We have extended the approach in [4], to MPLS Virtual Private Networks and have incorporated link based routing for QoS and BE classes of traffic. We have also extended the route based approach in [1] to accommodate MPLS VPN's and have modified the objective function. In the following sections we will explain the approach in [1] and [4] and our contribution in detail.

2.2.1 Route Based Routing

Traffic within a network can be differentiated into several classes depending on the kind of service required. A network should be able to accommodate and provide service for different classes of traffic. Different kinds of traffic require different constraints and grades

of service. To handle these end to end constraints the concept of admissible route sets is introduced in [1]. The admissible route sets are specific to each QoS service class s and to each origin-destination pair σ and are denoted as $R(s, \sigma)$. For each class that requires QoS, an admissible route set is pre-determined for a specific origin- destination (OD) pair and the final routes for routing are selected from this route set. Real-time services such as voice and video are sensitive to delay and hence require admissible route sets which are restricted in their hop number, while for a delay insensitive service class such as data traffic the admissible route set could have a less stringent hop restriction. Based on the service classes, traffic can be differentiated into high priority Quality of Service (QoS) traffic and low priority Best Effort (BE) traffic. The routing of high priority QoS traffic is not affected by the presence of the Best Effort traffic. Admissibility of a route depends on factors such as link capacities, available bandwidth, ability of nodes to handle certain services, administrative policies, etc., The concept of route based routing for a single data network was introduced in [1]. We will discuss this concept in detail and show our extension of this approach to MPLS Virtual Private Networks.

- **Network Model and Problem Formulation**

Consider a connected network with N nodes and L links with each link having a capacity C_l. The group of service classes that require QoS are denoted as S_{QoS}. Each individual class is denoted by s. $s \in S_{QoS}$. Let the network be represented by a graph $G = (V, E)$, where V is the set of all vertices that represent the nodes in the network and E is the set of all edges representing the links in the network.For each class s, we consider a $N \times N$ matrix D_s of bandwidth demands from source node σ_i to destination node σ_j. The problem is formulated as a multi-commodity flow problem with the objective to maximize the network revenue subjected to various constraints. Additional notation is given in Table 2.1.

In [1], the network revenue for QoS traffic is defined as follows:

$$W_{QoS} = \sum_{s \in S_{QoS}} \sum_{\sigma} \sum_{r \in R(s,\sigma)} e_{s,r} X_{s,r}$$

where $e_{s,r}$ and $X_{s,r}$ are given in Table 2.1. The multi-commodity flow problem presented in [1] is described below.

MCF problem P1:

$$Maximize \;\; W_{QoS} = \sum_{s \in S_{QoS}} \sum_{\sigma} \sum_{r \in R(s,\sigma)} e_{s,r} X_{s,r} \tag{2.1}$$

subject to the constraints

$$\left.\begin{array}{l} \sum_{r \in R(s,\sigma)} X_{s,r} \leq D_{s,\sigma} \\ X_{s,r} \geq 0, \forall r \in R(s,\sigma) \end{array}\right\} \forall s \in S_{QoS}, \forall \sigma \tag{2.2}$$

$$\sum_{s \in S_{QoS}} \sum_{\sigma} \sum_{r \in R(s,\sigma): l \in r} X_{s,r} \leq C_l, \forall l \tag{2.3}$$

Table 2.1: Notation of MCF problem for route based routing of QoS traffic.

V	set of vertices (routers) in the network
E	set of edges (directed links) in the network
$G = (V, E)$	Representation of the network as a graph
$l \in E$	Link
C_l	Capacity on link l
$D_{s,\sigma}$	Bandwidth demand for class s and OD pair σ, $\sigma = (\sigma_i, \sigma_j)$
$R(s, \sigma)$	The pre-selected route set for class s and OD pair σ
S_{QoS}	The set of service classes for QoS traffic
$e_{s,r}$	The earning per unit of carried traffic for class s on route r
W_{QoS}	Network revenue for QoS traffic
$X_{s,r}$	Allocated bandwidth for class s on route r

In (2.1), the objective is to maximize the network revenue W_{QoS} which is the product of the earning rate per unit of carried traffic for class $s \in S_{QoS}$, on route $r \in R(s, \sigma)$ and the allocated bandwidth for a OD pair σ on the route r. The summation is taken over all classes $s \in S_{QoS}$, for all OD pairs σ in the network and for all routes $r \in R(s, \sigma)$. The constraint in (2.2) ensures that the carried bandwidth for class s and OD pair σ does not exceed the demand $D_{s,\sigma}$ for that class and that OD pair. It also ensures that the allocated bandwidths should be greater than zero i.e non-negative. The constraint in (2.3) ensures that the total carried bandwidth on a link l for all routes $r \in R(s, \sigma)$, for all OD pairs and for all classes $s \in S_{QoS}$ does not exceed C_l, the capacity of that link. The *MCF problem P1* is a linear programming problem and can be solved by using a linear programming package such as CPLEX [14] to obtain a solution.On solving the above problem we obtain the maximum revenue W^*_{QoS}.

In [1], Best Effort traffic is routed using link based routing. An explanation of the link based routing for QoS and Best Effort traffic provided in [4] are discussed below.

2.2.2 Link Based Routing

In link based routing, there are no pre-selected route sets for a specific class or for a particular origin destination pair. The MCF problem here attempts to determine the allocated bandwidth on the links in a network instead of the routes.

- **Network model and Problem Formulation for Best Effort Traffic**

The network model and problem formulation for link based routing of Best Effort traffic according to [1] and [4] is as follows. Consider a connected network with N nodes and L links with each link having a capacity C_l. Let the network be represented by a graph $G = (V, E)$, where V is the set of all vertices that represent the nodes in the network and

E is the set of all edges representing the links in the network. We consider a $N \times N$ matrix $D_{s,\sigma}$ of bandwidth demands from source node σ_i to destination node σ_j. The problem is formulated as a multi-commodity flow problem with the objective to maximize the network revenue subjected to various constraints.

$$W_{BE} = \sum_{\sigma} e_{BE,\sigma} F_{BE,\sigma},$$

where $F_{BE,\sigma}$ is the total Best Effort traffic carried for OD pair σ, and $e_{BE,\sigma}$ is the earning per unit of carried Best Effort traffic of OD pair σ.
The objective is to maximize the network revenue W_{BE}. The notation and the problem formulation are given in the following.

Table 2.2: Notation of MCF problem for link based routing of BE traffic.

W_{BE}	Network revenue for BE traffic
$e_{BE,\sigma}$	The earning per unit of carried BE traffic for OD pair σ
$F_{BE,\sigma}$	Total carried BE traffic for OD pair σ
$D_{BE,\sigma}$	Bandwidth demand of OD pair σ for BE traffic
$Y_{\sigma,l}$	Allocated bandwidth for OD pair σ on link l
C_l	Capacity of link l
$L_{in}(n)$	Set of links directed into node n
$L_{out}(n)$	Set of links directed out of node n
σ_i	Source node of OD pair σ
σ_j	Destination node of OD pair σ

MCF problem P2:

$$Maximize \;\; W_{BE} = \sum_{\sigma} e_{BE,\sigma} F_{BE,\sigma} \tag{2.4}$$

subject to

$$0 \leq F_{BE,\sigma} \leq D_{BE,\sigma}, \quad \forall \sigma \tag{2.5}$$

$$\sum_{l \in L_{in}(n)} Y_{\sigma,l} - \sum_{l \in L_{out}(n)} Y_{\sigma,l} = \left\{ \begin{array}{ll} F_{BE,\sigma} & \text{if } n = \sigma_j \\ -F_{BE,\sigma} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \forall n, \forall \sigma \tag{2.6}$$

$$Y_{\sigma,l} \geq 0, \quad \forall \sigma, \forall l \tag{2.7}$$

$$\sum_{\sigma} Y_{\sigma,l} \leq C_l, \quad \forall l \tag{2.8}$$

The objective function in (2.4) is the network revenue. The constraint in (2.5) ensures that the total carried traffic $F_{BE,\sigma}$ for OD pair σ does not exceed the demand $D_{BE,\sigma}$ for

that OD pair. Equation (2.6) is the flow conservation constraint. It ensures that the total incoming traffic equals the total outgoing traffic for all nodes except the source node σ_i and the destination node σ_j. The constraint in (2.7) ensures that the allocated bandwidths are all non-negative. (2.8) ensures that the total allocated bandwidths on link l does not exceed its capacity C_l.

The allocated bandwidth $Y_{\sigma,l}$ indicates the bandwidth allocated on each link l for each OD pair σ. It does not give the utilized paths. Multiple paths could share a single link. In order to determine the routes for the flow of traffic a procedure called flow decomposition is necessary. This procedure is repeated for all OD pairs and is as follows. Flow-decomposition:

1. Fix an OD pair σ.

2. A subgraph $\mathcal{N}'$ is generated by removing all the links l such that $Y_{\sigma,l} = 0$ and the remaining graph is denoted by $\mathcal{G}$. The BE traffic for OD pair σ uses only those links present in graph $\mathcal{G}$.

3. Trace a route r in $\mathcal{G}$ from the source σ_i to the destination σ_j using the depth first search method. Let $Y_{BE,r} = min_{l \in r} Y_{\sigma,l}$. Compute
   $F_{BE,\sigma} = F_{BE,\sigma} - Y_{BE,r}$,
   and
   $Y_{\sigma,l} = Y_{\sigma,l} - Y_{BE,r}, \forall l \in r$.

4. End if $F_{BE,\sigma} = 0$
   else goto 2

Repeat for all OD pairs σ. In [4] the flow decomposition procedure is modified such that the path with the maximum bandwidth is chosen from the source to the destination.

2.2.3 Label Constraint

In the above approach, there is no constraint on the number of Label Switched Paths that are set up for each OD pair. As a result, the label space becomes very large at the Label Switch Routers and this is undesirable. In [6], Applegate and Thorup proposed some algorithms to reduce the label space. Label constraint was introduced in [4] to overcome these drawbacks.

In order to constrain the label space, the number of incoming labels at a node has to be controlled. Since MPLS supports label merge,the number of incoming labels equals the number of outgoing labels. The traffic bifurcation and traffic non-bifurcation concepts introduced in [10] and [11] can be used to constrain the label space. This leads to a Mixed Integer Programming (MIP) problem. A parameter called granularity g ($0 \leq g \leq 1$) is introduced to control the splitting of traffic among multiple paths. Granularity specifies how coarsely the traffic is divided. For a granularity g, the traffic is split among $1/g$ paths.

Thus, by defining the granularity the splitting of traffic can be controlled and the label space can be restricted. The label constraint defined in [4] is as follows.

$$Y_{\sigma,l} = M_{\sigma,l} \times (D_{BE,\sigma} \times g), \quad \forall\sigma, \forall l \tag{2.9}$$

$$\sum_{\sigma} \sum_{l \in L_{in}(n)} M_{\sigma,l} \leq L_{max}(n), \quad \forall n \tag{2.10}$$

$$M_{\sigma,l} \in Z, \ \ where \ \ Z \ \ is \ \ the \ \ set \ \ of \ \ integers. \ \ 0 \leq M_{\sigma,l} \leq \lfloor 1/g \rfloor, \forall\sigma, \forall l \tag{2.11}$$

In (2.9), $(D_{BE,\sigma} \times g)$ is the basic unit of flow that can be allocated to $Y_{\sigma,l}$, and $M_{\sigma,l}$ is an integer variable corresponding to $Y_{\sigma,l}$. The constraint in (2.9) ensures that the traffic carried on link l for OD pair σ can only be an integer multiple of the basic unit of traffic $(D_{BE,\sigma} \times g)$. In (2.10), $L_{max}(n)$ is the maximum number of labels allowed on a node n. The constraint in (2.10) ensures the maximum number of incoming labels $\sum_{\sigma} \sum_{l \in L_{in}(n)} M_{\sigma,l}$ to a node n does not exceed the label bound $L_{max}(n)$.

When g is set to 1, the demand between an OD pair will not be split between multiple LSP's.A single path is used to carry the demand between the OD pair. When $g = 1$, $M_{\sigma,l}$ is 0 or 1 for all σ and for all l. If $g < 1$, the range of $M_{\sigma,l}$ increases. The demand can be split up to at most among $[1/g]$ different LSP's.

Adding the above label constraint to MCF problem $P2$, modifies it to a MIP problem. The MIP problem is similar to a LP problem except that in a LP problem some of the variables are constrained to be integers. Here $M_{\sigma,l}$ is an integer. One of the methods of solving a MIP problem is the branch and bound method. In this method the optimal solution is first found without the integer constraints. If the variables whose values are constrained to be integers already have integer values, then it stops. If one or more integer variables have non-integral values, one fractional variable is chosen for branching, and two new subproblems are generated where the variable is more tightly constrained. In the branch and bound method, a series of LP subproblems are solved, and a tree of subproblem is built. Solving such problems requires far more computing time than the same problem without any integer constraints. The commercial package CPLEX can be used to solve MIP problems. This approach however, is extremely time consuming. In Section 2.4, we propose a method for getting around the complexity of solving MIP problems.

2.2.4 Loop Elimination

The routing technique described in [1], could lead to the creation of loops within a network. These loops increase the network resource utilization without increasing the efficiency or the network revenue. The loops can be eliminated by modifying the objective function so as to account for the utilized resources. The modified objective function is given by:

$$MaximizeW_{BE} = \sum_{\sigma} e_{BE,\sigma} F_{BE,\sigma} - \varepsilon \sum_{\sigma} \sum_{l} Y_{\sigma,l} \tag{2.12}$$

In (2.12), the first term $\sum_\sigma e_{BE,\sigma} F_{BE,\sigma}$ is the total network revenue resulting from the carried traffic. The second term $\sum_\sigma \sum_l Y_{\sigma,l}$ is the total bandwidth or network resource consumed in the network and may be considered as the cost of carrying the traffic. If there are loops in the network the utilized resources would increase without increasing the network revenue.By accounting for the utilized resources in the network revenue, we penalize the network revenue and thus eliminate the loops in the network. The parameter ε must be chosen appropriately for the prevention of loops. The effect of ε is discussed later in Section 2.4.3.

The modified MCF including label constraint and loop elimination is given below.

MCF problem P3:

Input: G=(V,E), $0 \leq g \leq 1, D_{BE,\sigma}, \{C_l : l = 1, 2, ..., |E|\}, L_{max}(n), \varepsilon$

$$maximize \;\; W_{BE} = \sum_\sigma e_{BE,\sigma} F_{BE,\sigma} - \varepsilon \sum_\sigma \sum_l Y_{\sigma,l} \tag{2.13}$$

subject to

$$0 \leq F_{BE,\sigma} \leq D_{BE,\sigma}, \quad \forall \sigma$$

$$\sum_{l \in L_{in}(n)} Y_{\sigma,l} - \sum_{l \in L_{out}(n)} Y_{\sigma,l} = \left\{ \begin{array}{ll} F_{BE,\sigma} & \text{if } n = \sigma_j \\ -F_{BE,\sigma} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \forall n, \forall \sigma$$

$$Y_{\sigma,l} = M_{\sigma,l} \times (D_{BE,\sigma} \times g), \quad \forall \sigma, \forall l$$

$$\sum_\sigma Y_{\sigma,l} \leq C_l, \quad \forall l$$

Label limitation:

$$\sum_\sigma \sum_{l \in L_{in}(n)} M_{\sigma,l} \leq L_{max}(n), \forall n$$

$$M_{\sigma,l} \in Z, where \;\; Z \;\; is \;\; the \;\; set \;\; of \;\; integers, \;\; 0 \leq M_{\sigma,l} \leq \lfloor 1/g \rfloor, \forall \sigma, \forall l$$

In the objective function (2.13), we reduce the network revenue by accounting for the utilization of resources and thus eliminate loops in the network. The other constraints are as explained earlier.

Problem Formulation for Link Based QoS Routing

QoS traffic can be differentiated into several classes depending on the kind of service required. Each class is assigned a different earning rate $e_{s,\sigma}$. The class that has a higher earning rate $e_{s,\sigma}$ has a higher precedence than that with a lower earning rate. The traffic flow for a lower class cannot preempt that of a higher class. The constraints imposed in MCF problem $P3$ hold good for QoS traffic also. An additional hop constraint is imposed so as to limit the number of hops in the route [4],[8]. For the hop constraint to be effective,

a non- bifurcation problem is considered i.e the granularity g is set to 1. The hop constraint is as follows.

$$\sum_{l} Y^{s}_{\sigma,l} \leq H_{max}(s) \times D^{s}_{\sigma} \tag{2.14}$$

In (2.15), $H_{max}(s)$ is the maximum number of hops for the traffic of class s. D^{s}_{σ} is the traffic demand for class s and OD pair σ. $Y^{s}_{\sigma,l}$ is the allocated bandwidth on link l, for class s and OD pair σ. Since it is a non-bifurcation problem, the traffic does not split among multiple paths and the bandwidth allocated on link l for OD pair σ and class s, $Y^{s}_{\sigma,l}$ is either D^{s}_{σ} or zero. By ensuring that the allocated bandwidth for OD pair σ and class s on all the network links does not exceed $H_{max}(s) \times D^{s}_{\sigma}$, we ensure that the length of the path for this OD pair does not exceed $H_{max}(s)$.

The formulation of the MCF problem for the QoS traffic as in [4] is given below. Additional notations are given in Table 2.3.

Table 2.3: Notation of MCF problem with Hop Constraint.

$e_{s,\sigma}$	The earning per unit carried traffic for class s and OD pair σ
F^{s}_{σ}	Total carried traffic for class s and OD pair σ
D^{s}_{σ}	Bandwidth demand for class s and OD pair σ
$Y^{s}_{\sigma,l}$	Allocated bandwidth for class s and OD pair σ on link l
$H_{max}(s)$	Allocated bandwidth for class s and OD pair σ on link l

MCF problem P4:

$$Maximize \;\; W_{QoS} = \sum_{s,\sigma} e_{s,\sigma} F^{s}_{\sigma} - \varepsilon \sum_{s,\sigma} \sum_{l} Y^{s}_{\sigma,l}$$

subject to

$$0 \leq F^{s}_{\sigma} \leq D^{s}_{\sigma}, \quad \forall \sigma, \forall s$$

$$\sum_{l \in L_{in}(n)} Y^{s}_{\sigma,l} - \sum_{l \in L_{out}(n)} Y^{s}_{\sigma,l} = \left\{ \begin{array}{ll} F^{s}_{\sigma} & \text{if } n = \sigma_j \\ -F^{s}_{\sigma} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \forall n, \forall \sigma, \forall s$$

$$\sum_{l} Y^{s}_{\sigma,l} \leq H_{max}(s) \times D^{s}_{\sigma}, \quad \forall s, \sigma$$

$$Y^{s}_{\sigma,l} = M^{s}_{\sigma,l} \times D^{s}_{\sigma}, \quad \forall \sigma, \forall l, \forall s$$

$$\sum_{s} \sum_{\sigma} Y^{s}_{\sigma,l} \leq C_l, \quad \forall l$$

$$0 \leq M^{s}_{\sigma,l} \leq 1$$

2.3 Our Approach to Traffic Engineering in MPLS VPN's

In this section we propose our model for traffic engineering of QoS and Best Effort traffic in MPLS VPN's.In section 2.3.1, the MCF problem for route based routing in a MPLS VPN is explained. The link based routing approach for QoS traffic are discussed in detail in section 2.3.2. Traffic bifurcation in MPLS VPN's and hop constraint is also presented in this section. The link based routing approach for BE traffic are discussed in detail in section 2.3.3.Our experimental results showing the effect of various parameters is presented in section 2.4.

2.3.1 Route Based Routing of QoS Traffic for MPLS VPN's

The concept of route based routing for a single data network has been explained earlier in section 2.2.1. We have extended this algorithm to accommodate MPLS VPN's and also modified the objective function to account for utilization of network resources.

- **Network Model and Problem Formulation**

Consider a connected network with N nodes and L links with each link having a capacity C_l. Let T be the set of all VPN's which is defined as $T = t1, t2, t3, ...$ The group of service classes that require QoS are denoted by S_{QoS}. Each individual class is denoted by s. $s \in S_{QoS}$. Let the network be represented by a graph $G = (V, E)$, where V is the set of all vertices that represent the nodes in the network and E is the set of all edges representing the links in the network.For each class s, we consider a $N \times N$ matrix D_s of bandwidth demands from source node σ_i to destination node σ_j. The problem is formulated as a multi-commodity flow problem with the objective to maximize the network revenue subjected to various constraints.Additional notation is given in Table 2.4.

The network revenue for route based routing for QoS traffic is given as:

$$W_{QoS} = \sum_{s \in S_{QoS}} \sum_{t} \sum_{\sigma} \sum_{r_\sigma^t \in R(s,\sigma^t)} e_{s,r_\sigma^t} P_{s,r_\sigma^t} - \epsilon \sum_{s \in S_{QoS}} \sum_{t} \sum_{\sigma} \sum_{r_\sigma^t} \sum_{l} e_{s,r_\sigma^t} P^l_{s,r_\sigma^t} \tag{2.15}$$

The MCF problem P5 for route based routing of QoS traffic is as follows.

MCF problem P5:

$$Maximize \;\; W_{QoS} = \sum_{s \in S_{QoS}} \sum_{t} \sum_{\sigma} \sum_{r_\sigma^t \in R(s,\sigma^t)} e_{s,r_\sigma^t} P_{s,r_\sigma^t} - \epsilon \sum_{s \in S_{QoS}} \sum_{t} \sum_{\sigma} \sum_{r_\sigma^t} \sum_{l} e_{s,r_\sigma^t} P^l_{s,r_\sigma^t} \tag{2.16}$$

subject to the constraints

$$\left.\begin{array}{l} \sum_{r_\sigma^t \in R(s,\sigma^t)} P_{s,r_\sigma^t} \leq D_{s,\sigma^t} \\ P_{s,r_\sigma^t} \geq 0, \forall r \in R(s,\sigma) \end{array}\right\}, \forall s \in S_{QoS}, \forall \sigma, \forall t \tag{2.17}$$

Table 2.4: Notation of MCF problem with route based routing in MPLS VPNs.

σ^t	OD pair with source node σ_i and destination node σ_j for VPN t
r_σ^t	Route for OD pair σ and VPN t
$R(s,\sigma^t)$	Admissible route set for class s, OD pair σ and VPN t, $r_\sigma^t \in R(s,\sigma^t)$
e_{s,r_σ^t}	earning per unit of carried traffic for class s , route r, OD pair σ and VPN t
P_{s,r_σ^t}	allocated bandwidth for class s, route r, OD pair σ and VPN t
P^l_{s,r_σ^t}	allocated bandwidth for class s , route r, OD pair σ and VPN t on link l
D_{s,σ^t}	demand for class s, OD pair σ and VPN t
W_{QoS}	Network revenue for QoS traffic

$$\sum_{s\in S_{QoS}} \sum_{t} \sum_{\sigma} \sum_{r_\sigma^t \in R(s,\sigma^t): l\in r} P_{s,r_\sigma^t} \leq C_l, \forall l \tag{2.18}$$

The objective is to maximize the network revenue given by (2.16). The first term in (2.16) represents the total network revenue as a result of carrying the traffic. It is the product of the earning rate per unit of carried QoS traffic for a particular OD pair and the carried traffic for that class and OD pair. The second term in (2.16) accounts for the utilization of resources. P^l_{s,r_σ^t} is the carried traffic on a single link l. A longer route has more links than a shorter one. The different classes $s \in S_{QoS}$ are assigned different earning rates e_{s,r_σ^t} with a higher rate being assigned to the high priority traffic. The second term in (2.16) has to be as small as possible in order to maximize the network revenue. By including the earning rate in the second term we ensure that the routes for high priority traffic are shorter than those of low priority traffic. W_{QoS} which is the sum of the earnings over all classes $s \in S_{QoS}$, all VPN's in T ,all OD pairs σ and over all routes $r \in R(s,\sigma)$ indicates the total network revenue. The constraint in (2.17) ensures that the carried bandwidth for class s ,VPN t and OD pair σ does not exceed the demand D_{s,σ^t} for that class and that OD pair. It also ensures that the allocated bandwidths should be greater than zero i.e non-negative. The constraint in (2.18) ensures that the total carried bandwidth on a link l for all routes $r_\sigma^t \in R(s,\sigma^t)$, for all VPN's T, for all OD pairs σ and for all classes $s \in S_{QoS}$ that utilize a link l does not exceed C_l, the capacity of that link. The *MCF problem P5* is a linear programming problem and can be solved by using a commercial linear programming package such as CPLEX [13] to obtain a solution.On solving the above problem we obtain the maximum revenue W^*_{QoS}.

2.3.2 Link Based Routing of QoS Traffic

Our approach to link based routing of QoS traffic is presented in this section. The MCF problems in [4] are extended to support MPLS Virtual Private Networks.

- **Network Model and Problem Formulation for Link Based QoS Routing**

Consider a connected network with N nodes and L links with each link having a capacity C_l. Let T be the set of all VPN's which is defined as $T = t1, t2, t3, ...$ The group of service classes that require QoS are denoted by S_{QoS}. Each individual class is denoted by s. $s \in S_{QoS}$. Let the network be represented by a graph $G = (V, E)$, where V is the set of all vertices that represent the nodes in the network and E is the set of all edges representing the links in the network.For each class s, we consider a $N \times N$ matrix D_s of bandwidth demands from source node σ_i to destination node σ_j. The problem is formulated as a multi-commodity flow problem with the objective to maximize the network revenue subjected to various constraints. Additional notation is given in the table below

Table 2.5: Notations for link based routing of QoS traffic in MPLS VPNs.

σ^t	origin destination pair with source i, destination j for vpn t, $\sigma = (\sigma_i, \sigma_j)$
g	Granularity- controls number of LSP's
e_{s,σ^t}	earning per unit of carried traffic for class s and OD pair σ in vpn t
F_{s,σ^t}	carried traffic for class s and OD pair σ in vpn t
D_{s,σ^t}	demand for class s and OD pair σ in vpn t
Y^l_{s,σ^t}	allocated traffic for class s and OD pair σ in vpn t on link l
M^l_{s,σ^t}	integer variable corresponding to Y^l_{s,σ^t}
C_l	Capacity of link l
$L_{in(n)}$	set of links incoming into node n
$L_{out(n)}$	set of links outgoing from node n

The MCF problem P6 for link based QoS routing is given below. The network revenue for link based routing for QoS traffic is given as:

$$W_{QoS} = \sum_s \sum_t \sum_\sigma e_{s,\sigma^t} F_{s,\sigma^t} - \epsilon \sum_s \sum_t \sum_\sigma \sum_l Y^l_{s,\sigma^t} \tag{2.19}$$

MCF problem P6:

$$Maximize \;\; W_{QoS} = \sum_s \sum_t \sum_\sigma e_{s,\sigma^t} F_{s,\sigma^t} - \epsilon \sum_s \sum_t \sum_\sigma \sum_l Y^l_{s,\sigma^t} \tag{2.20}$$

subject to the constraints

$$0 \leq F_{s,\sigma^t} \leq D_{s,\sigma^t} \;\; \forall \sigma, \forall t, \forall s \tag{2.21}$$

$$\sum_{l \in L_{in}(n)} Y^l_{s,\sigma^t} - \sum_{l \in L_{out}(n)} Y^l_{s,\sigma^t} = \left\{ \begin{array}{ll} F_{s,\sigma^t} & \text{if } n = \sigma_j \\ -F_{s,\sigma^t} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \;\; \forall n, \forall \sigma, \forall t, \forall s \tag{2.22}$$

$$\sum_s \sum_t \sum_\sigma Y^l_{s,\sigma^t} \leq C_l \;\; \forall l \tag{2.23}$$

(2.20) represents the total network revenue. The first term in (2.20) represents the total network reward as a result of carrying the traffic. It is the product of the earning rate per unit of carried QoS traffic and the carried traffic for that class.The second term in (2.20) accounts for the utilization of resources. Y^l_{s,σ^t} is the allocated traffic on a single link l for class s and OD pair σ^t. The second term can be viewed as the cost of carrying the traffic and this is subtracted from the network revenue to account for the utilized resources.If the utilized bandwidth is increased without increasing the network revenue, as in the case of loops in the network, the network revenue is penalized. The constraint in (2.21) ensures that the carried bandwidth for class s ,VPN t and OD pair σ does not exceed the demand D_{s,σ^t} for that class and that OD pair and also that the carried bandwidth is greater than zero i.e nonnegative. The constraint in (2.22) is the flow conservation constraint. It ensures that the total incoming traffic equals the total outgoing traffic for all nodes except the source node σ_i and destination node σ_j. (2.23) ensures that the total traffic carried on a particular link l for all classes s, for all OD pairs and all VPN's does not exceed the capacity of that link. The *MCF problem P6* is a linear programming problem and can be solved by using a commercial linear programming package such as CPLEX [13] to obtain a solution.On solving the above problem we obtain the maximum revenue W^*_{QoS}.

- **Traffic Bifurcation in MPLS VPN's**

In order to constrain the label space and prevent large routing tables at the routers we use the traffic bifurcation technique discussed in section 2.2.4.

The traffic bifurcation constraint for MPLS VPN's is :

$$Y^l_{s,\sigma^t} = M^l_{s,\sigma^t} \times (D_{s,\sigma^t} \times g), \quad \forall\sigma, \forall t, \forall s, \forall l \tag{2.24}$$

$$0 \leq M^l_{s,\sigma^t} \leq \lfloor 1/g \rfloor, \quad \forall\sigma, \forall t, \forall s, \forall l \tag{2.25}$$

$$M^l_{s,\sigma^t} \in Z, \quad where \;\; Z \;\; is \;\; the \;\; set \;\; of \;\; integers. \tag{2.26}$$

In (2.24), $(D_{s,\sigma^t} \times g)$ is the basic unit of flow that can be allocated to Y^l_{s,σ^t}, and M^l_{s,σ^t} is an integer variable corresponding to Y^l_{s,σ^t}. The constraint in (2.24) ensures that the traffic carried on link l for OD pair σ can only be an integer multiple of the basic unit of traffic $(D_{BE,\sigma^t} \times g)$.

When g is set to 1, the demand between an OD pair will not be split between multiple LSP's. A single path is used to carry the demand between the OD pair. When $g = 1$, M^l_{s,σ^t} is 0 or 1 for all σ and for all l. If $g < 1$, the range of M^l_{s,σ^t} increases. The demand can be split up to at most among $[1/g]$ different LSP's. The MCF problem along with the traffic bifurcation constraint is given below.

MCF problem P7:

$$Maximize \;\; W_{QoS} = \sum_s \sum_t \sum_\sigma e_{s,\sigma^t} F_{s,\sigma^t} - \epsilon \sum_s \sum_t \sum_\sigma \sum_l Y^l_{s,\sigma^t} \tag{2.27}$$

subject to the constraints

$$0 \leq F_{s,\sigma^t} \leq D_{s,\sigma^t} \quad \forall\sigma, \forall t, \forall s \tag{2.28}$$

$$\sum_{l \in L_{in}(n)} Y^l_{s,\sigma^t} - \sum_{l \in L_{out}(n)} Y^l_{s,\sigma^t} = \left\{ \begin{array}{ll} F_{s,\sigma^t} & \text{if } n = \sigma_j \\ -F_{s,\sigma^t} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \quad \forall n, \forall\sigma, \forall t, \forall s \tag{2.29}$$

$$Y^l_{s,\sigma^t} = M^l_{s,\sigma^t} \times (D_{s,\sigma^t} \times g), \quad \forall\sigma, \forall t, \forall s, \forall l \tag{2.30}$$

$$0 \leq M^l_{s,\sigma^t} \leq \lfloor 1/g \rfloor, \quad \forall\sigma, \forall t, \forall s, \forall l \tag{2.31}$$

$$M^l_{s,\sigma^t} \in Z, \quad where \;\; Z \;\; is \;\; the \;\; set \;\; of \;\; integers. \tag{2.32}$$

$$\sum_s \sum_t \sum_\sigma Y^l_{s,\sigma^t} \leq C_l, \quad \forall l \tag{2.33}$$

(2.30) augments the problem to a Mixed Integer Programming problem as $M^s_{\sigma,l}$ is an integer. The above problem is solved using CPLEX with the LP-to-Integer method.

- **Hop Constraint in MPLS VPN's**

As mentioned earlier, differentiation of VPN traffic can be done by choosing earning rates for all the classes of traffic. The class with a higher earning rate receives a higher priority compared to other classes that have a lower earning rate. The hop constraint discussed in section [2.2.6] is extended to MPLS VPN's. The hop constraint for MPLS VPN's is given below.

$$\sum_l Y^l_{s,\sigma^t} \leq H_{max}(s) \times D_{s,\sigma^t}, \quad \forall s, \forall\sigma, \forall t \tag{2.34}$$

In (2.31), $H_{max}(s)$ is the maximum number of hops for the traffic of class s. D_{s,σ^t} is the traffic demand for class s and OD pair σ. Y^l_{s,σ^t} is the allocated bandwidth on link l, for class s and OD pair σ. We treat this is as a non-bifurcation problem and set the granularity to 1. As a result, the traffic does not split among multiple paths and the bandwidth allocated on link l for OD pair σ and class s, Y^l_{s,σ^t} is either D_{s,σ^t} or zero. By ensuring that the allocated bandwidth for OD pair σ and class s on all the network links does not exceed $H_{max}(s) \times D_{s,\sigma^t}$, we ensure that the length of the path for this OD pair does not exceed $H_{max}(s)$. The MCF problem P8 with the hop constraint for QoS routing is given below.

MCF problem P8:

$$Maximize \;\; W_{QoS} = \sum_s \sum_t \sum_\sigma e_{s,\sigma^t} F_{s,\sigma^t} - \epsilon \sum_s \sum_t \sum_\sigma \sum_l Y^l_{s,\sigma^t} \tag{2.35}$$

subject to the constraints subject to

$$0 \leq F_{s,\sigma^t} \leq D_{s,\sigma^t}, \quad \forall\sigma, \forall t, \forall s \tag{2.36}$$

$$\sum_{l \in L_{in}(n)} Y^l_{s,\sigma^t} - \sum_{l \in L_{out}(n)} Y^l_{s,\sigma^t} = \left\{ \begin{array}{ll} F_{s,\sigma^t} & \text{if } n = \sigma_j \\ -F_{s,\sigma^t} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \forall n, \forall\sigma, \forall t, \forall s \tag{2.37}$$

$$\sum_{l} Y^{l}_{s,\sigma^t} \leq H_{max}(s) \times D_{s,\sigma^t}, \quad \forall s, \forall \sigma, \forall t \tag{2.38}$$

$$Y^{l}_{s,\sigma^t} = M^{l}_{s,\sigma^t} \times (D_{s,\sigma^t} \times g), \quad \forall \sigma, \forall t, \forall s, \forall l \tag{2.39}$$

$$0 \leq M^{l}_{s,\sigma^t} \leq \lfloor 1/g \rfloor, \quad \forall \sigma, \forall t, \forall s, \forall l \tag{2.40}$$

$$M^{l}_{s,\sigma^t} \in Z, \quad where \ \ Z \ \ is \ \ the \ \ set \ \ of \ \ integers. \tag{2.41}$$

$$\sum_{s} \sum_{t} \sum_{\sigma} Y^{l}_{s,\sigma^t} \leq C_l, \quad \forall l \tag{2.42}$$

2.3.3 Link Based Routing of Best Effort Traffic

Our approach to link based routing of BE traffic is presented in this section. The MCF problems in [4] are extended to support MPLS Virtual Private Networks.

- **Network Model and Problem Formulation for Link Based BE traffic Routing**

Consider a connected network with N nodes and L links with each link having a capacity C_l. Let T be the set of all VPN's which is defined as $T = t1, t2, t3, ...$ Here we consider only a single class of traffic i.e Best Effort. Let the network be represented by a graph $G = (V, E)$, where V is the set of all vertices that represent the nodes in the network and E is the set of all edges representing the links in the network.We consider a $N \times N$ matrix D_{BE} of bandwidth demands from source node σ_i to destination node σ_j. The problem is formulated as a multi-commodity flow problem with the objective to maximize the network revenue subjected to various constraints. Additional notation is given in Table 2.6.

Table 2.6: Notation of MCF problem for link based routing of BE traffic in MPLS VPNs.

σ^t	origin destination pair with source i, destination j for vpn t, $\sigma = (\sigma_i, \sigma_j)$
g	Granularity- controls number of LSP's
e_{BE,σ^t}	earning per unit of carried BE traffic for OD pair σ in vpn t
F_{BE,σ^t}	carried traffic for class BE and OD pair σ in vpn t
D_{BE,σ^t}	demand for class BE and OD pair σ in vpn t
Y^{l}_{BE,σ^t}	allocated traffic for class BE and OD pair σ in vpn $t$on link l
C_l	Capacity of link l
$L_{in(n)}$	set of links incoming into node n
$L_{out(n)}$	set of links outgoing from node n
M^{l}_{BE,σ^t}	integer variable corresponding to Y^{l}_{BE,σ^t}

The MCF problem P9 for link based routing of BE traffic is given below. The network revenue for link based routing for BE traffic is given as:

$$W_{BE} = \sum_t \sum_\sigma e_{BE,\sigma^t} F_{BE,\sigma^t} - \epsilon \sum_t \sum_\sigma \sum_l Y^l_{BE,\sigma^t} \tag{2.43}$$

MCF problem P9:

$$Maximize \;\; W_{QoS} = \sum_t \sum_\sigma e_{BE,\sigma^t} F_{BE,\sigma^t} - \epsilon \sum_t \sum_\sigma \sum_l Y^l_{BE,\sigma^t} \tag{2.44}$$

subject to the constraints

$$0 \leq F_{BE,\sigma^t} \leq D_{BE,\sigma^t}, \quad \forall\sigma, \forall t \tag{2.45}$$

$$\sum_\sigma \sum_{l \in L_{in}(n)} Y^l_{BE,\sigma^t} - \sum_\sigma \sum_{l \in L_{out}(n)} Y^l_{BE,\sigma^t} = \left\{ \begin{array}{ll} F_{BE,\sigma^t} & \text{if } n = \sigma_j \\ -F_{BE,\sigma^t} & \text{if } n = \sigma_i \\ 0 & otherwise \end{array} \right\} \forall n, \forall\sigma, \forall t \tag{2.46}$$

$$Y^l_{BE,\sigma^t} = M^l_{BE,\sigma^t} \times (D_{BE,\sigma^t} \times g), \quad \forall\sigma, \forall t, \forall l \tag{2.47}$$

$$0 \leq M^l_{BE,\sigma^t} \leq [1/g], \quad \forall\sigma, \forall t, \forall l$$

$$M^l_{BE,\sigma^t} \in Z, \;\; where \;\; Z \;\; is \;\; the \;\; set \;\; of \;\; integers. \tag{2.48}$$

$$\sum_t \sum_\sigma Y^l_{BE,\sigma^t} \leq C_l, \quad \forall l \tag{2.49}$$

The MCF problem formulation is similar to that of QoS with the exception of the hop constraint. There is no hop constraint imposed on the routing of Best Effort traffic. (2.41) represents the total network revenue. The first term in (2.41) represents the total network reward and the second term in (2.41) accounts for the utilization of resources. The constraint in (2.42) ensures that the carried bandwidth for Best Effort does not exceed the demand D_{BE,σ^t} for that OD pair and also that the carried bandwidth is greater than zero i.e nonnegative. The constraint in (2.43) is the flow conservation constraint. (2.44) ensures that the carried traffic is always an integer multiple of the basic unit of traffic. (2.46) ensures that the total traffic carried on a particular link l for class Best Effort for all OD pairs and all VPN's does not exceed the capacity of that link. The *MCF problem P9* is a linear programming problem and is solved by using a linear programming package such as CPLEX [13] to obtain a solution. On solving the above problem we obtain the maximum revenue W^*_{QoS}.

2.4 Experimental Results

In this section, we present our experimental results. In Section 2.4.1, we describe the networks used in our simulations. The method of generation of synthetic networks is

described. In Section 2.4.2 the results for route based routing of QoS traffic are presented. In Section 2.4.3, the effect of parameters like ϵ, granularity and the earning rate are shown. The results for onestage and twostage routing for all three networks are also presented. The LP-to-Integer method and its comparison with the LP method is also presented.

2.4.1 Networks

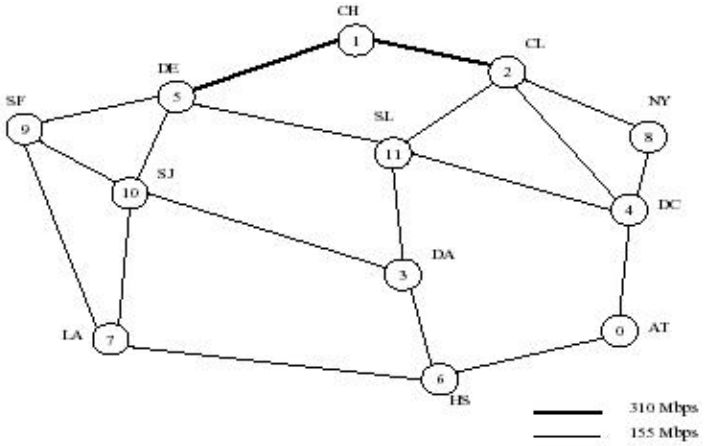

Figure 2.1: Abstract US network

In this experiment, two types of networks are considered. The first one is the abstract US backbone network which has a fixed topology. The network has 12 nodes and 38 edges. The network topology along with link capacities are shown in Figure 2.1. We consider the US network as network 1 in all our simulations.

The second type of networks are randomly generated by a graph generator GT-ITM [10] to produce synthetic 2-level networks. The 2-level networks are used to simulate the hierarchical networks. The construction of the network topology is as follows. In the first level, a connected graph is generated with the given node number inside a unit square as in Figure 2.2. In the second level, the nodes of the first level which are denoted as cluster are replaced by a smaller connected graph which is generated inside a unit square with the given node number. The first level edges are typically longer than the second level edges. We have generated two hierarchical networks. One has 18 nodes and 62 edges and is considered as network 2. The other hierarchical network has 30 nodes and 94 edges and is considered as network 3.

The individual VPNs for each of these networks are generated by the user. The size of the VPN, the OD pairs for the VPN and the number of VPN's are specified by the user. The demand for each OD pair for a given VPN is generated as described in [6]. The method is based on the Euclidean distance of the OD pair. The graph generator randomly places the nodes in a unit square. The distance $\delta(x, y)$ between two nodes x and y is

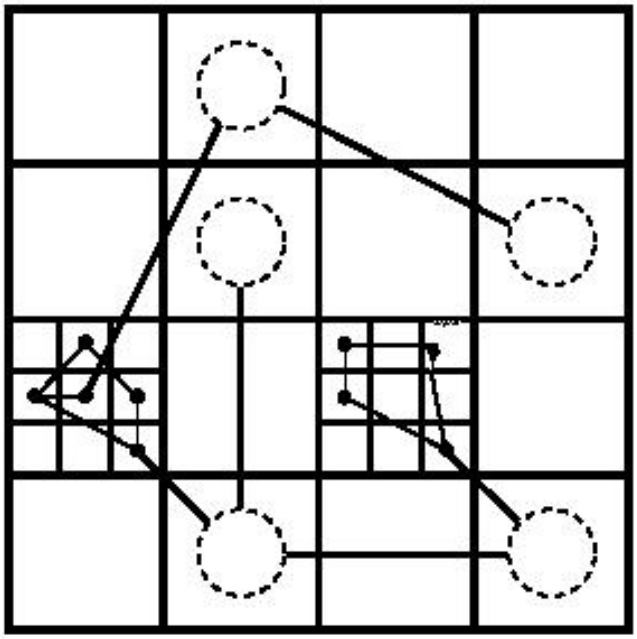

Figure 2.2: 2 level Hierarchical Topology

obtained from their coordinates. For node x, we generate two random numbers o_x, $d_x \in$ [0,1]. Similarly, for node y, we have o_y, $d_y \in$ [0,1]. For each OD pair (x, y), we pick a random number $c_{(x,y)} \in$ [0,1]. Then the demand between x and y is given by

$$\alpha o_x d_y c_{(x,y)} e^{-\delta(x,y)/2\triangle} \tag{2.50}$$

Here α is the parameter that controls the maximum demand and $\triangle$ is the largest Euclidean distance between any pair of nodes. This method generates more demand between pairs of nodes that have a smaller distance than those that have a longer distance. The networks generated by GT-ITM are listed as in Table 2.7.

Table 2.7: Networks generated by two level Hierarchical Topology.

Network	Number of Nodes	Number of Edges
network 2	18	62
network 3	30	94

2.4.2 Experimental results for route based routing

In this section we present the results for route based routing of QoS traffic. We have implemented route based routing only for the US network as it has a fixed topology and it is possible to specify certain admissible route sets for each OD pair. We specified two VPN's each with 3 OD pairs and each OD pair having 3 routes between them. The results are shown in Figures 2.3 and 2.4. We plot the percentage of carried traffic vs. percentage of demand for both VPN's and both classes of traffic. The percentage of carried traffic for each class for a individual VPN is also plotted. It can be seen that Class A has a higher percentage of carried traffic when compared to Class B. This is due to the higher earning rate of Class A which gives it a higher priority and it also generates a higher network revenue.The average hop number for each class is also shown. It is seen that Class B has a higher average hop number than Class A. This shows that a shorter route is being chosen for Class A when compared to Class B.

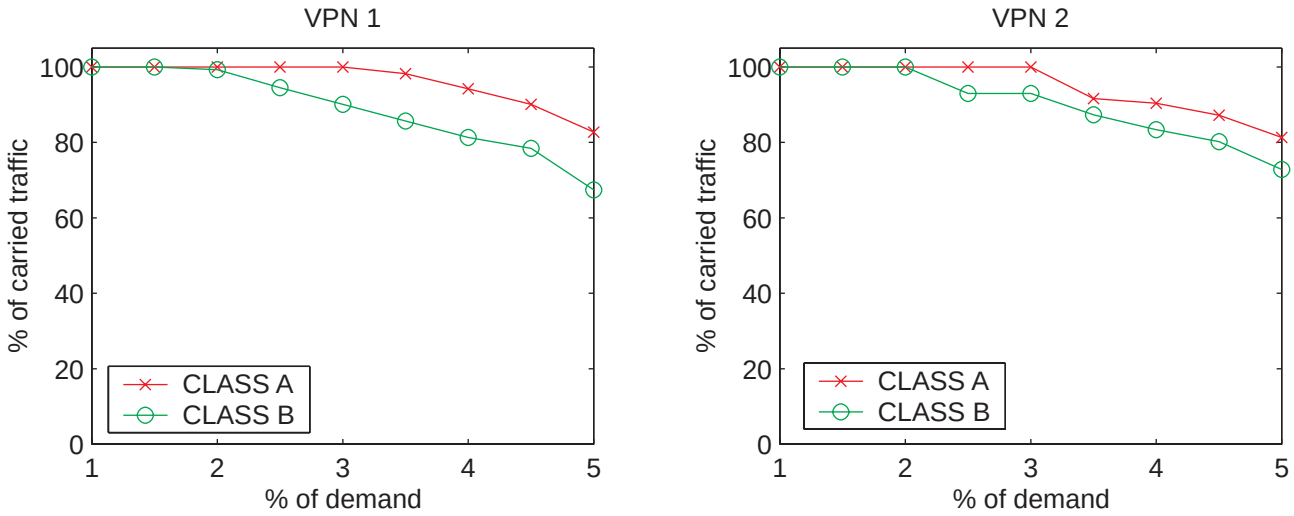

Figure 2.3: Route based routing

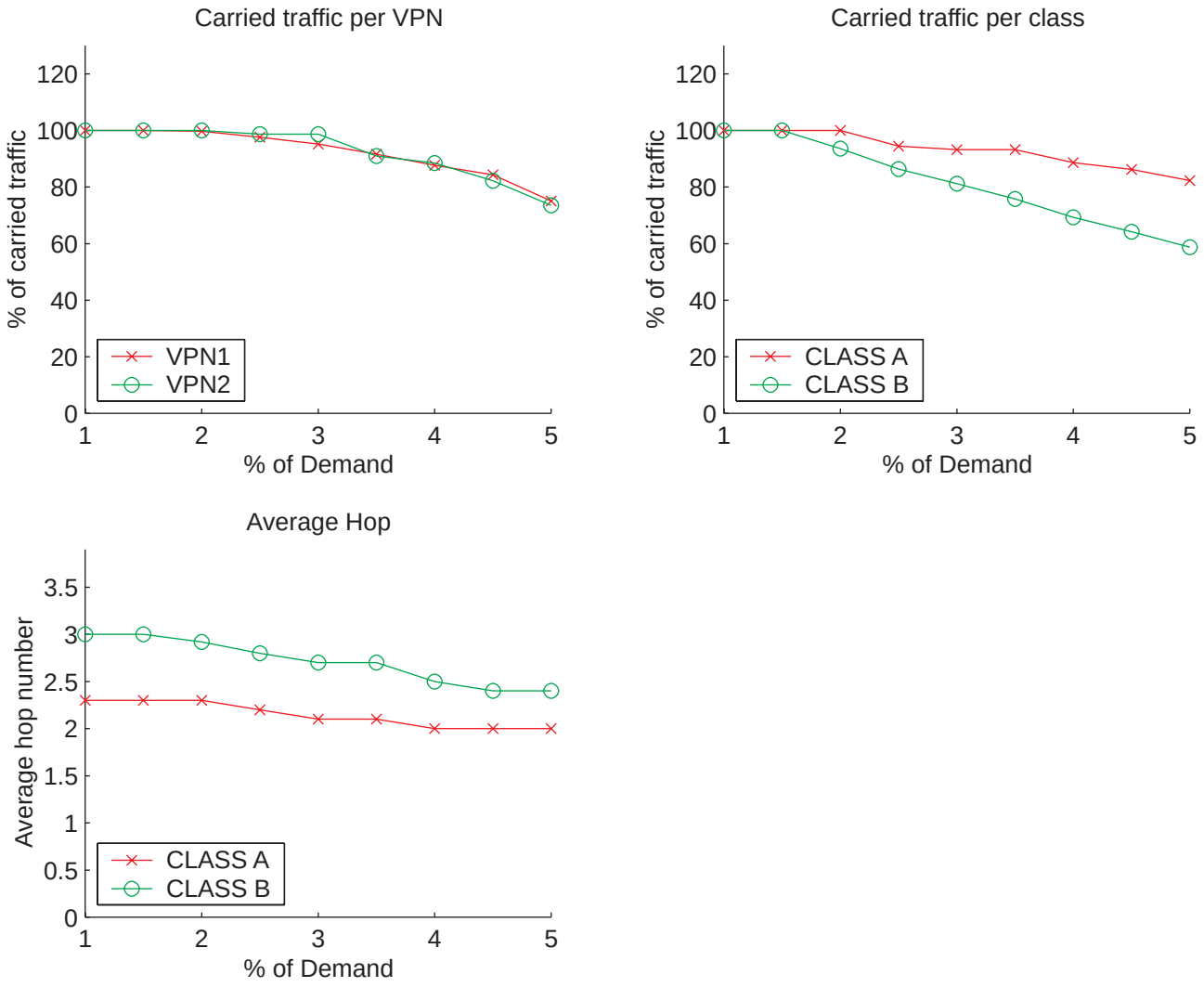

Figure 2.4: Route based routing

2.4.3 Experimental results for link based routing

- **Effect of ϵ**

In this section, we show the effect of varying ϵ in networks 1, 2 and 3 and also identify its proper range. We compare the network resources, the percentage of carried traffic, the total number of paths, and the number of loops for different values of ϵ. The earning rate e_{s,σ^t} is set to one for all VPNs, so that the carried traffic is maximized in the network.

Since the sum of allocated bandwidth Y^l_{s,σ^t} is greater than the total carried traffic $\sum_\sigma F_{s,\sigma^t}$ over all the OD pairs σ for all VPN's t the ϵ should be small enough,so that the second term in the objective function is as small as possible and the network revenue is maximized. If ϵ is set to zero, it has the same effect as removing the utilized resource from the network revenue and this will create loops in the network.

In Figures 2.5-2.7 we plot the network resources, percentage of carried traffic, the total number of paths, and the total number of loops vs the value of ε for each of the three networks. The percentage of the carried traffic is defined as the ratio of carried traffic to the traffic demand. It can be seen in some cases from the figures as ε is close to zero or equal to zero, loops are created in the network. But as ε increases from zero, the number of loops decreases and reaches 0 for ε in the range of 10^{-6} to 10^{-2}. As the number of loops decreases, the utilized resources in the network also decreases. But, the percentage of carried traffic and total number of paths remains unchanged. For large values of ε, (e.g, $\varepsilon > 0.01$) the carried traffic, the number of paths, and the utilized resources all decrease rapidly. This is due to the fact that as ϵ increases, the cost of carrying the traffic increases compared to the network reward. In order to maximize the network revenue, the percentage of carried traffic is reduced for large values of ϵ.Very large values of ε should therefore be avoided.

- **Granularity**

In this section, we show the effect of granularity on the total carried traffic for all the three networks. The problem is treated as a MIP problem due to the integer constraint in equation (2.38) and is solved using CPLEX. The carried traffic plotted in Figure 2.8 is the largest amount that the given network can carry for the given value of granularity g. For a given granularity g, the demand for an OD pair can be split among $\lfloor 1/g \rfloor$ different paths. Consequently, if the value of g is very large, the routing conditions will be more stringent, and may result in lesser carried traffic. However, from Figure 2.8 it is seen that this effect is small and the carried traffic does not vary significantly with the choice of granularity g.

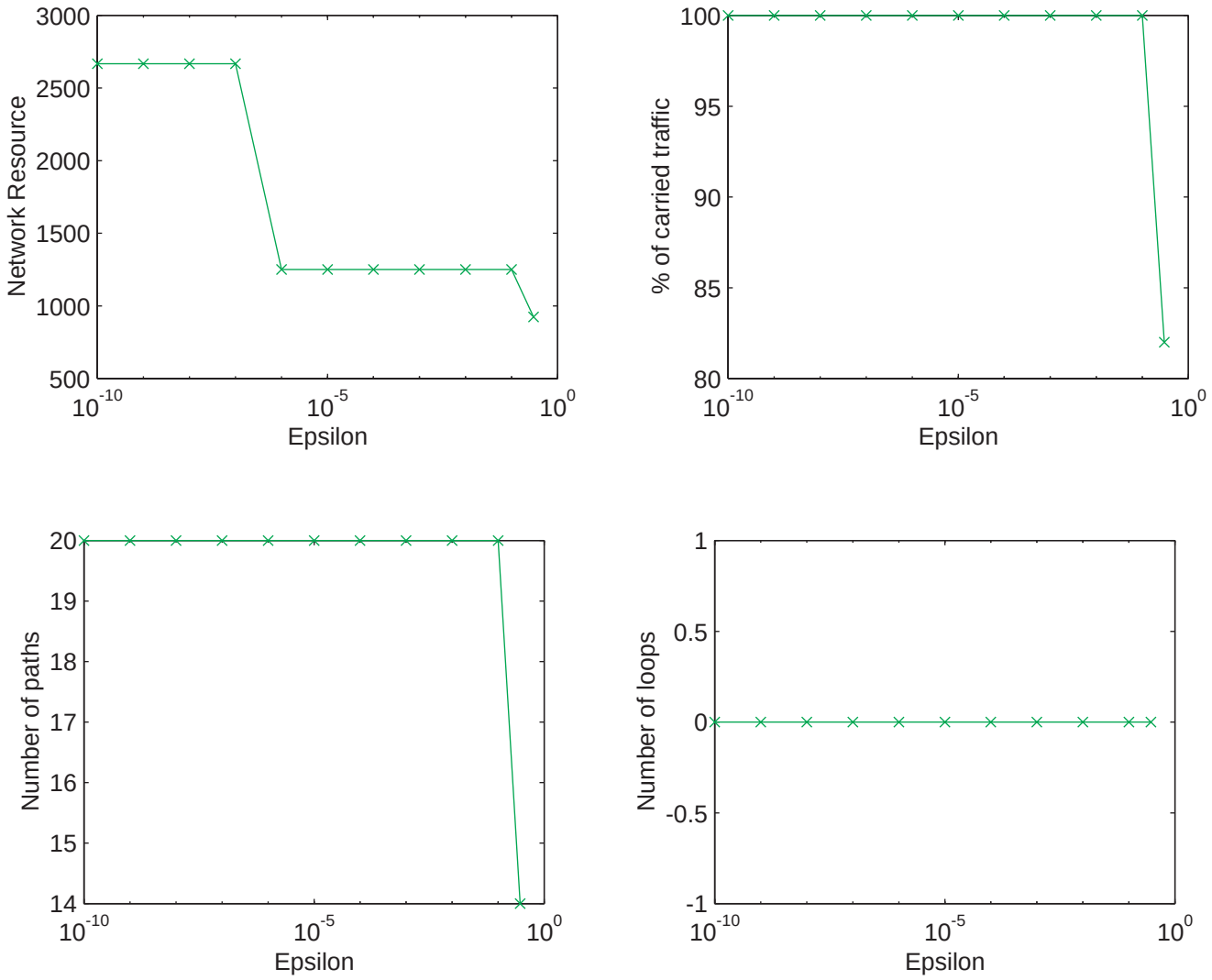

Figure 2.5: Effect of Epsilon in Network 1

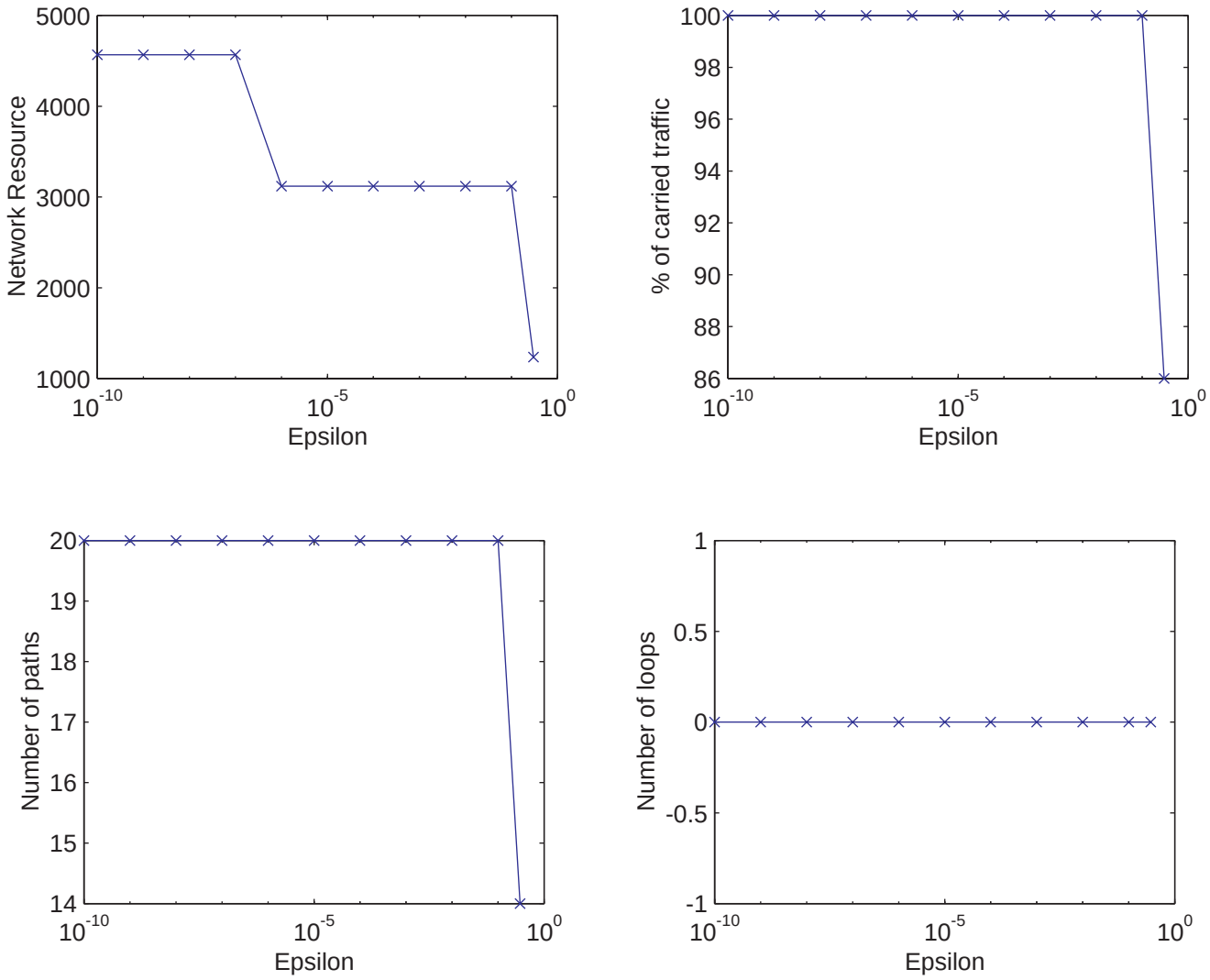

Figure 2.6: Effect of Epsilon for Network 2

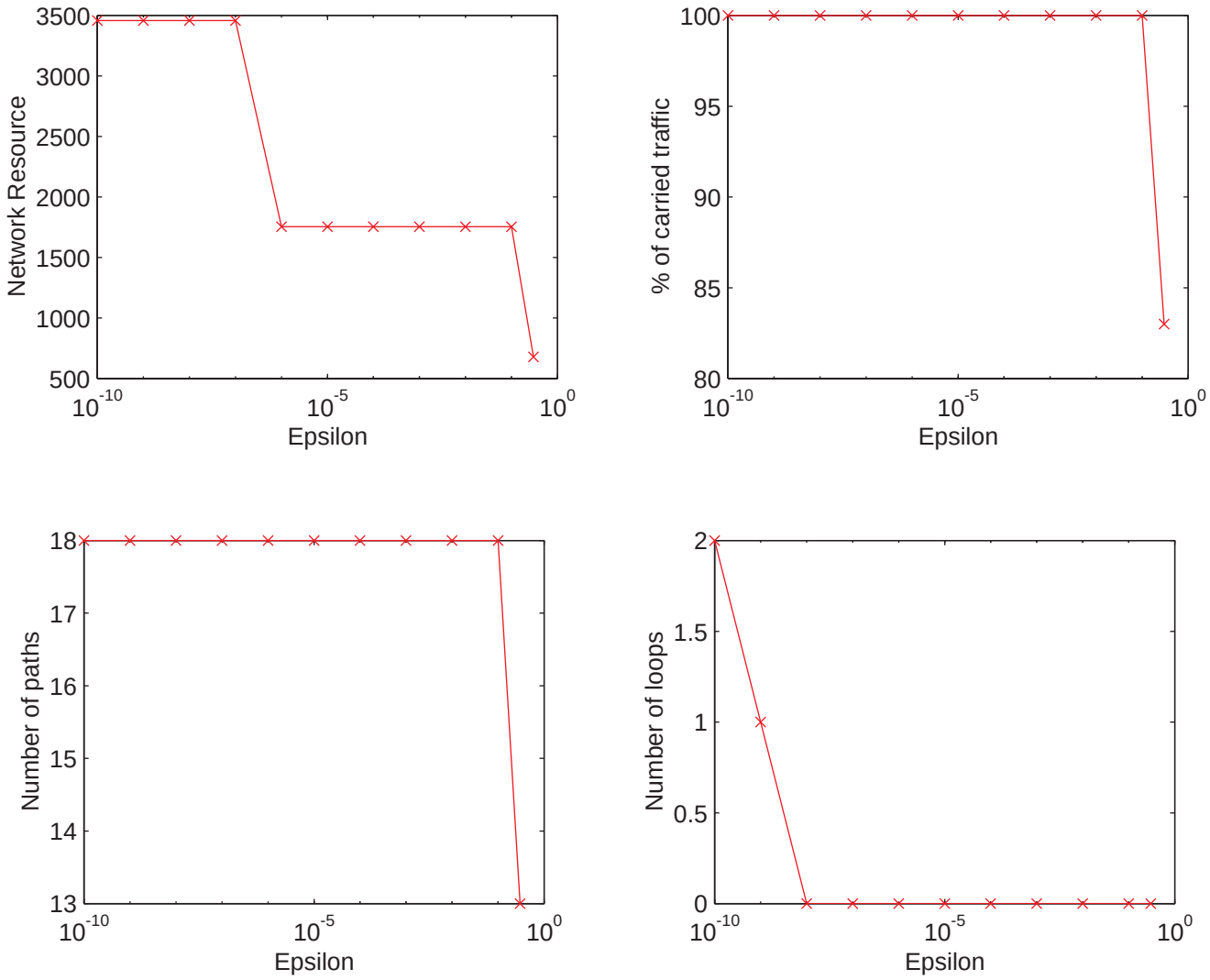

Figure 2.7: Effect of Epsilon in Network 3

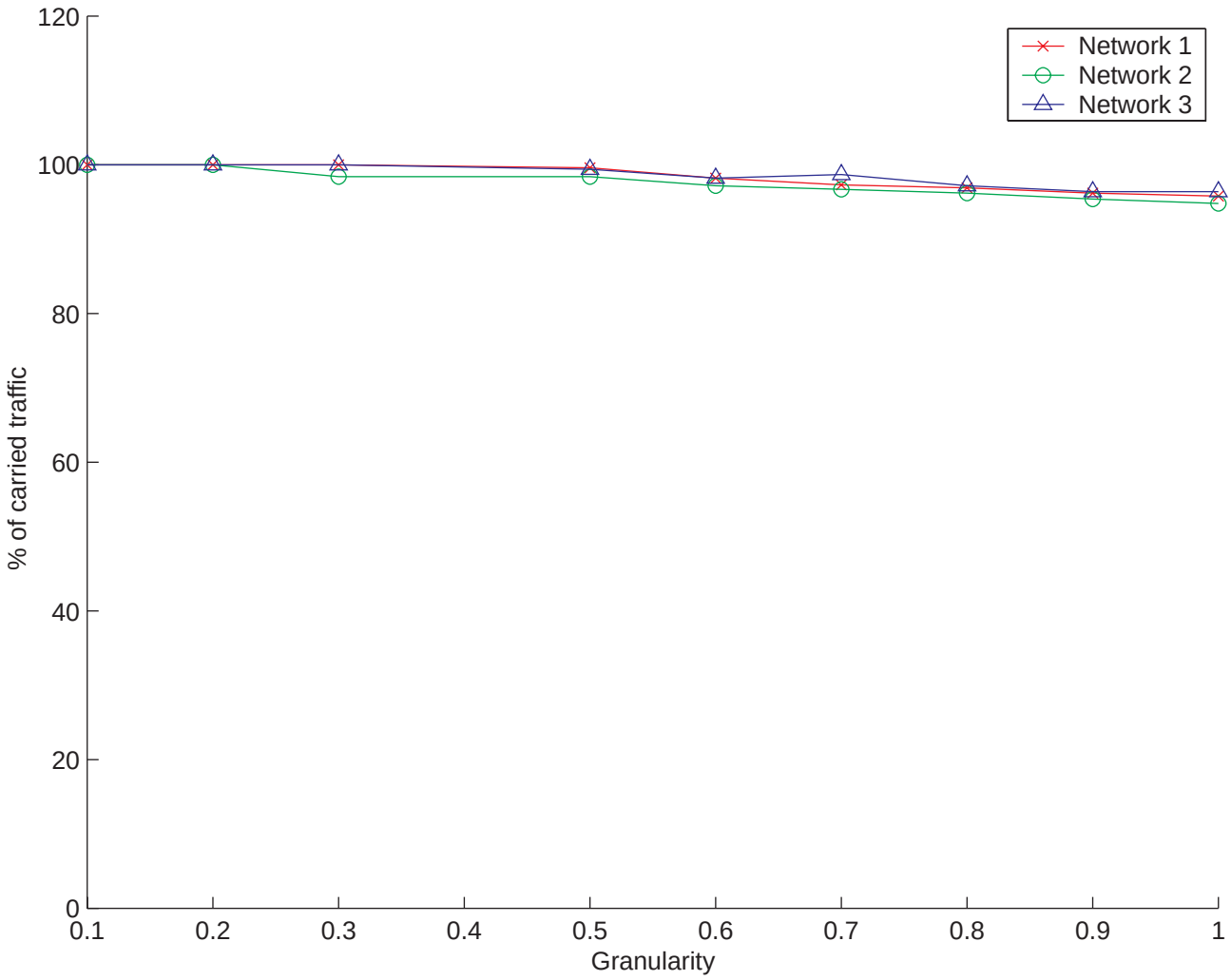

Figure 2.8: Effect of granularity

In Figure 2.9 we show the effect of granularity for varying demand. It is seen that when *granularity* is set to 1, for varying demand the percentage of carried traffic is low. When *granularity* is set to 0.5, the percentage of carried traffic increases and is highest when *granularity* is set to 0.1. This is because when granularity is set to 0.1 the traffic is split among [1/0.1] multiple paths.

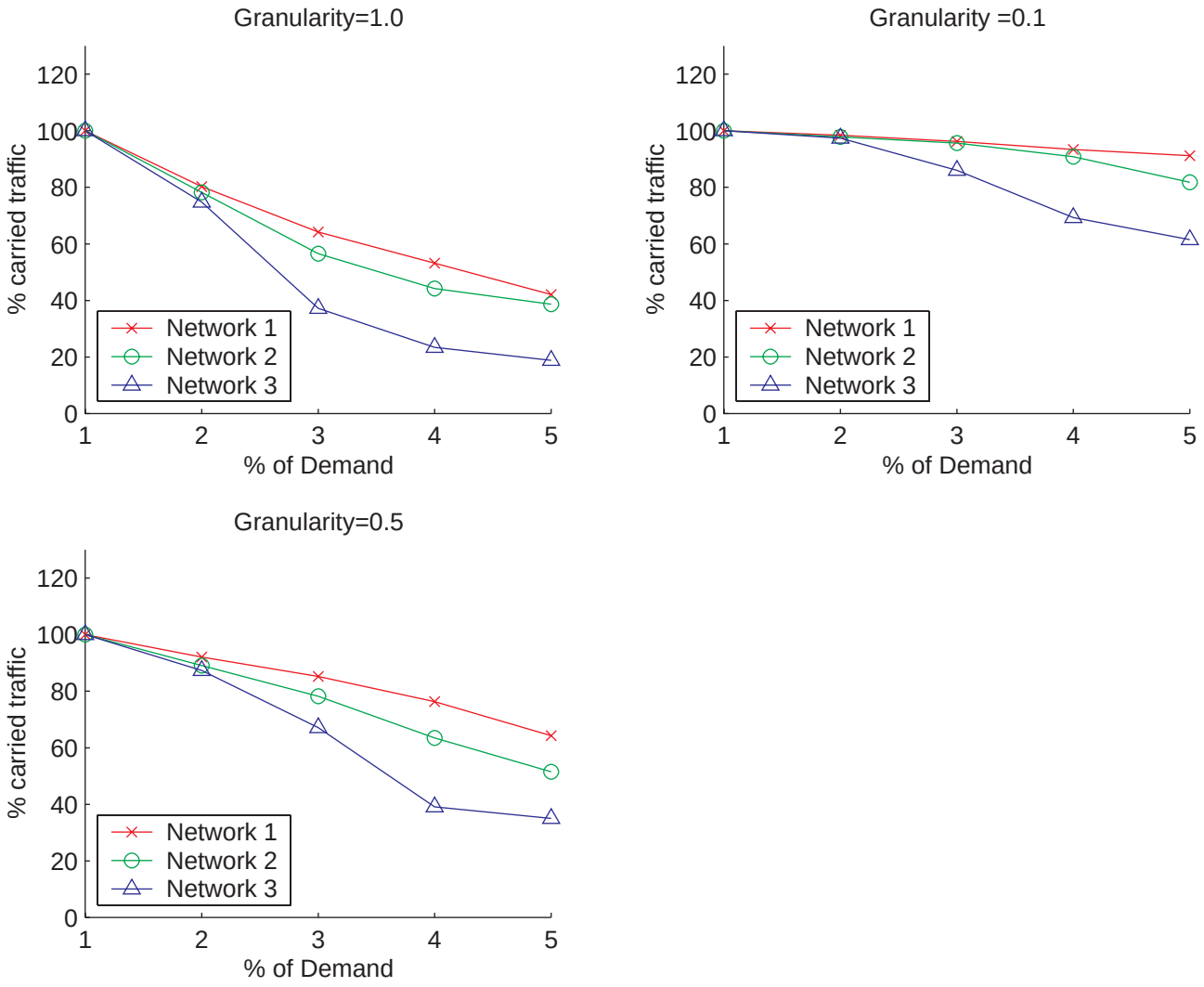

Figure 2.9: Effect of granularity with varying overload

- **LP to Integer Approach**

As discussed earlier, MIP problems are computationally extensive and complex. Therefore we try to find a solution which is computationally less complex, although the solution may not be optimal. Such a suboptimal solution will be acceptable only if it's performance is close to that of the optimal solution. Since most demands can be satisfied in one or two routes, we propose an approach that seeks an LP solution first and later modifies it to obtain a MIP solution. We first solve the original MIP problem, but do not enforce the variables M^l_{s,σ^t} to be integer. As a result,M^l_{s,σ^t} may be a real number. We then round down M^l_{s,σ^t} to the nearest integer to obtain a MIP solution.

In this section, we compare the difference of the LP-to-Integer approach and the LP approach for all the three networks. The granularity g is set to one to study the worst case performance. In this case, if the demand is split, the traffic demand will be dropped by the LP-to-Integer approach. We plot the combined traffic demands of all VPNs's in a network. In Figure 2.10 we plot the percentage of carried traffic vs the value of alpha. The parameter α controls the amount of the demands as described in Section 2.4.1. As α increases, demands between OD pairs also increases but the percentage of carried traffic drops. It can be seen that the LP-to-Integer approach does not carry as much traffic as LP approach in the worst case, but it stays quite close to the LP. The biggest gap between the LP-to-Integer and LP approach is around 4%. This is quite acceptable for saving a lot of computational time when compared to the MIP problem.

- **Effect of Earning Rates**

In this section, we illustrate the effect of the earning rate e_{s,σ^t} on the priorities of routing traffic. We assign different earning rates for the three classes of traffic namely Class A, Class B and Best Effort. We perform the experiment on all the networks considering that all three networks carry all three classes of traffic. The QoS and BE traffic of each network are routed together. The different service classes are differentiated by the values of e_{s,σ^t} . The graphs show the plot of the percentage of carried traffic vs the percentage of demand for different earning rates of all three classes.

The Figures 2.11, 2.12 and 2.13, show the effect of earning rate e_{s,σ^t} for network 1, network2 and network 3 respectively. We tested the effect of earning rate by setting the values for Class A, Class B and BE as $(1, 1, 1), (30, 20, 1), (90, 20, 1), (90, 60, 30)$. It can be seen that all the three classes have a different drop precedence. Since the earning rate for Class A is higher when compared to Class B and BE it is dropped to a much lesser degree. BE traffic receives lowest priority. As we increase the demand, the traffic class with the lowest earning rates starts dropping.

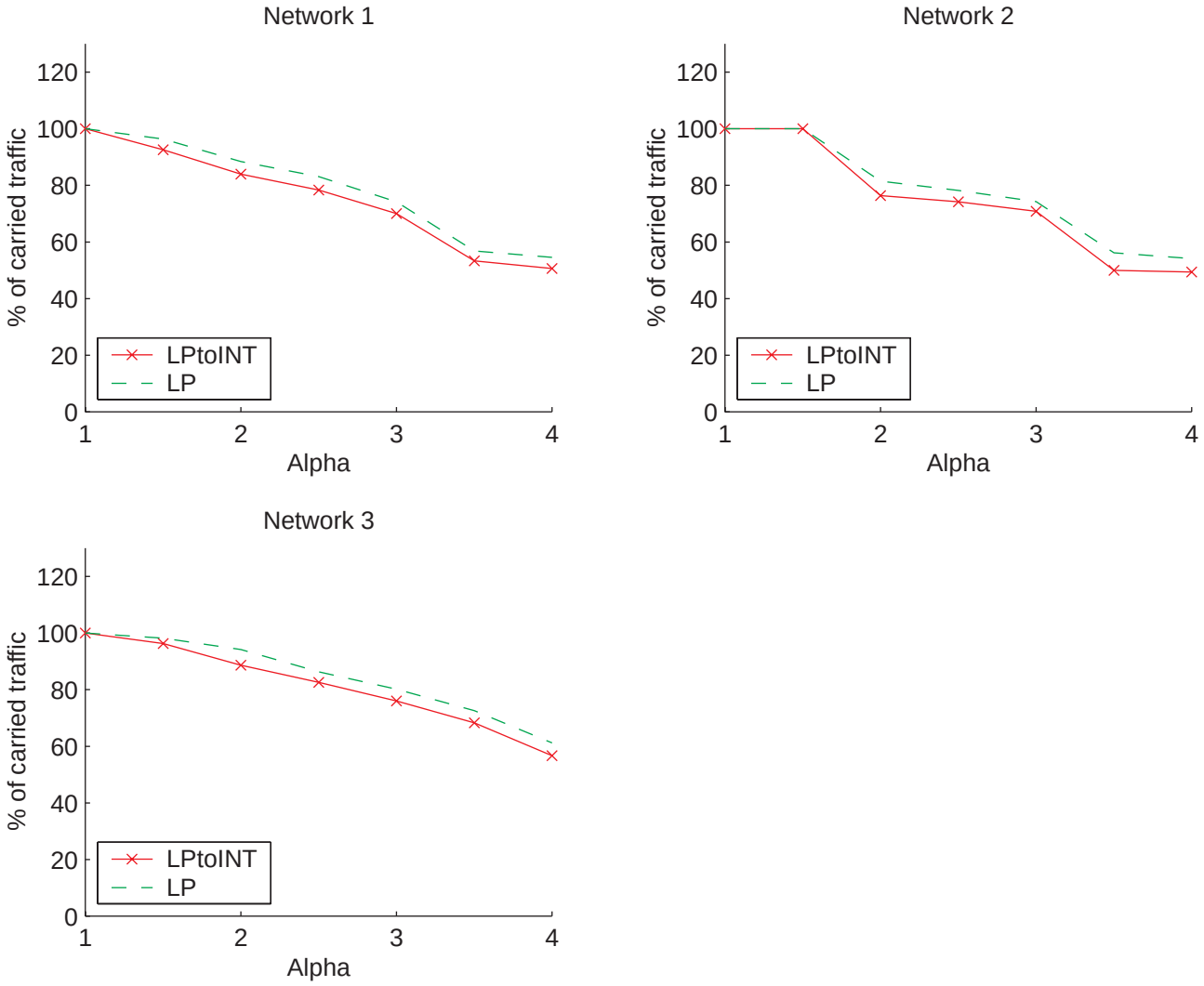

Figure 2.10: Comparison of LP and LP-to-INT for all networks

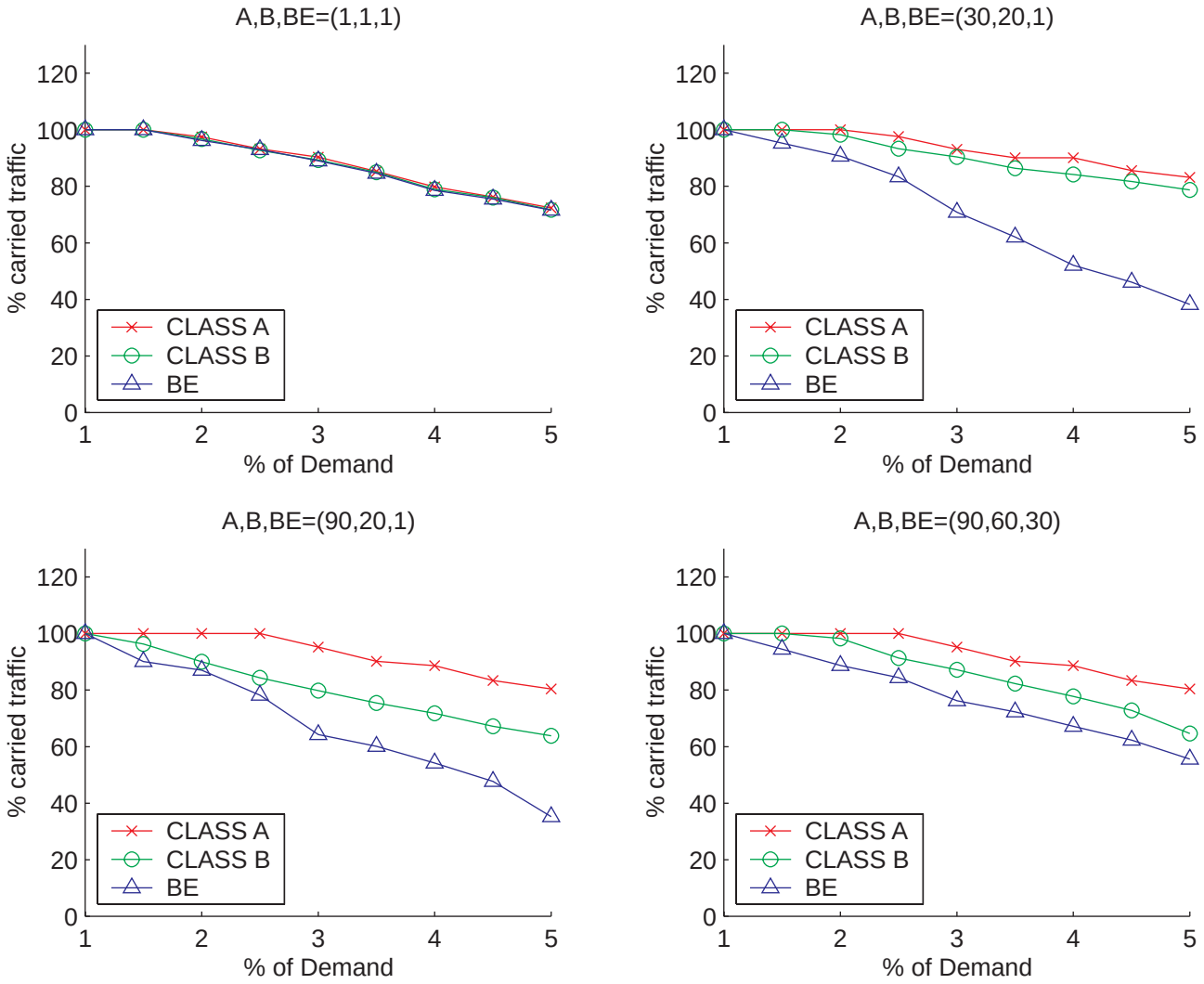

Figure 2.11: Effect of earning rate for Network 1

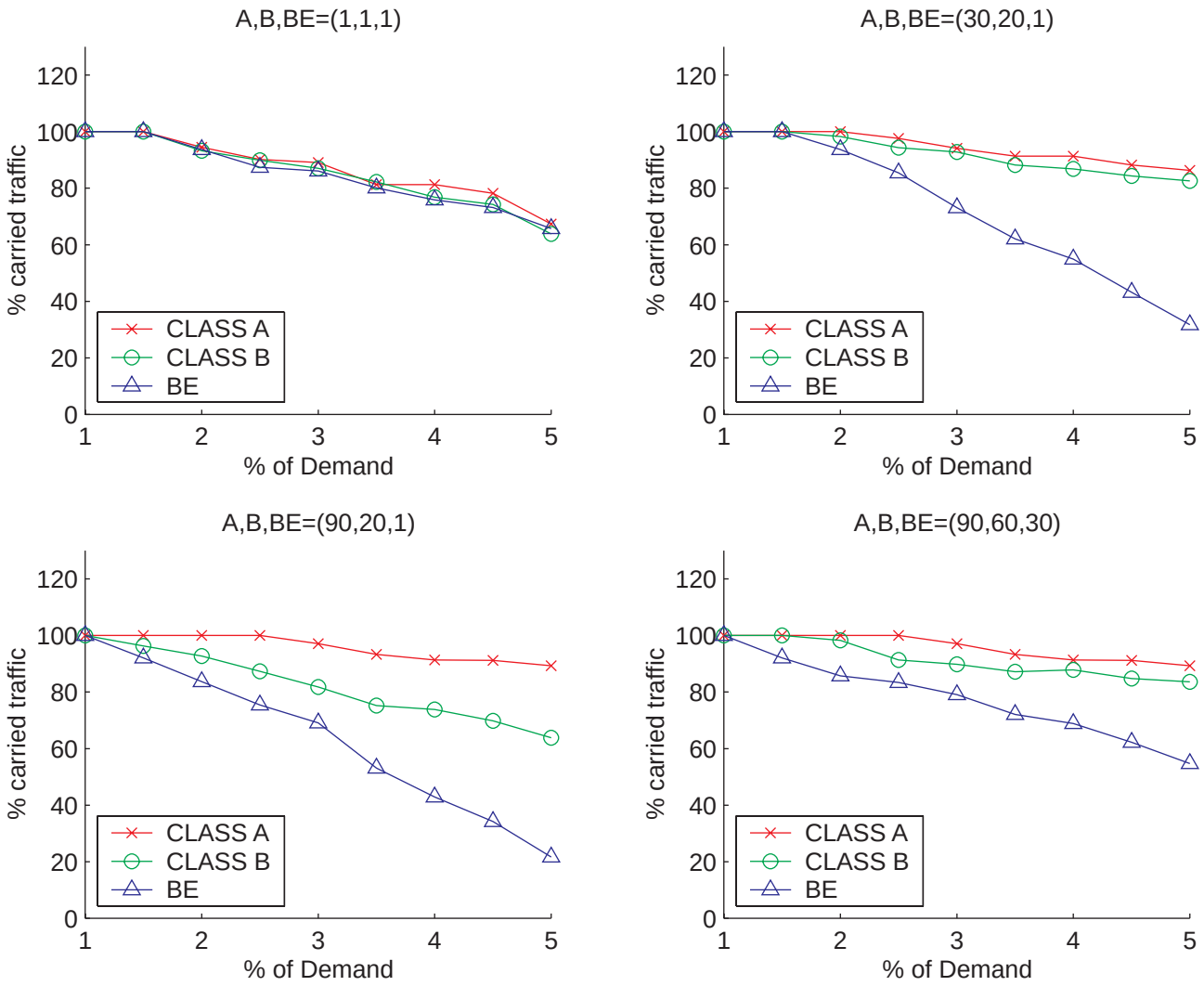

Figure 2.12: Effect of earning rate for Network 2

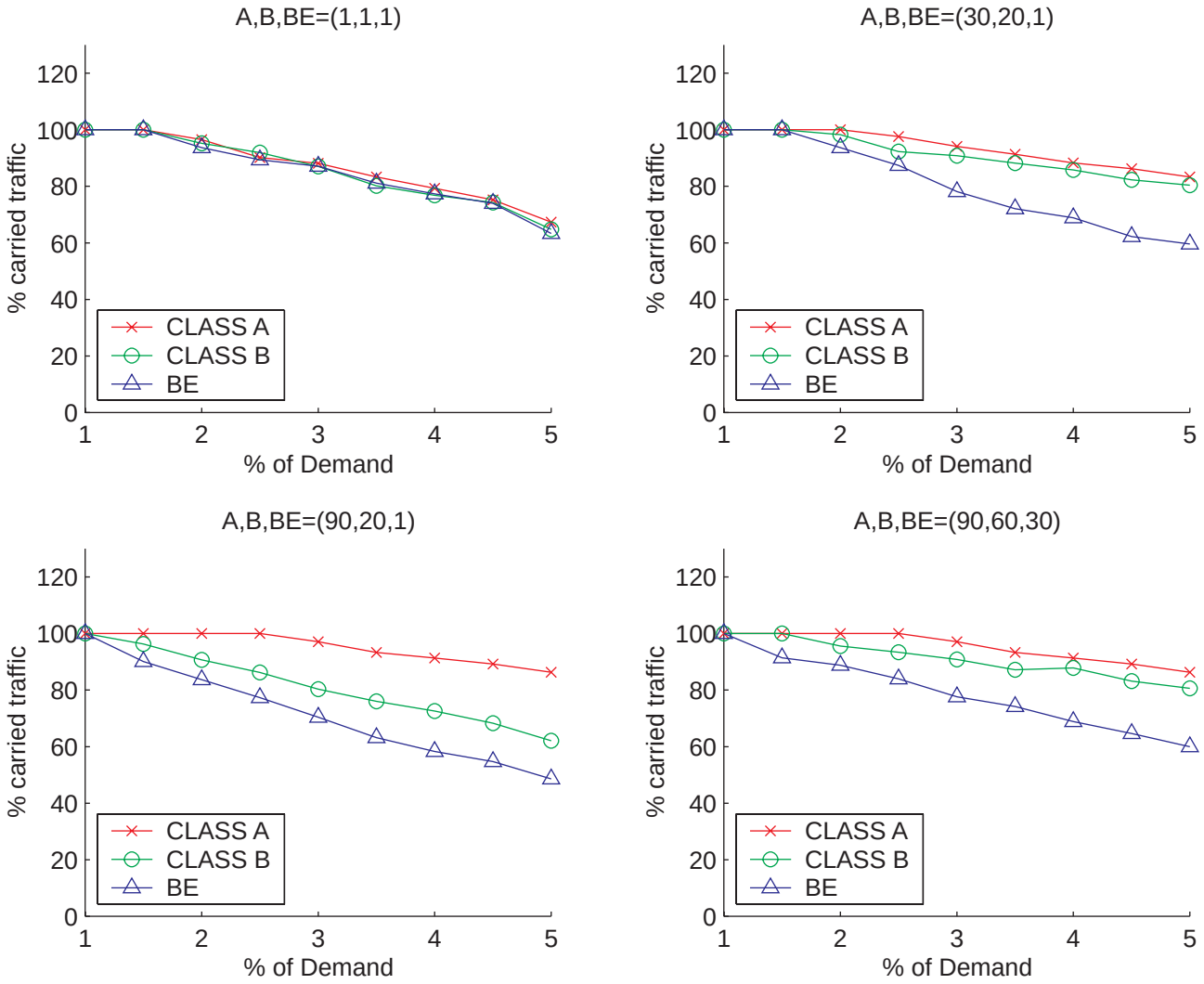

Figure 2.13: Effect of earning rate for Network 3

- **Onestage and Twostage Routing**

In this section we further show the effect of earning rate e_{s,σ^t} by routing the traffic in two different methods. In the first case, referred to as one stage routing, the high priority QoS traffic and the low priority BE traffic are routed together. We plot the percentage of carried traffic and the average hop number vs the percentage of demand for all the three networks. The different earning rates for all the classes results in a different drop precedence. In this case, BE traffic is dropped faster than the QoS traffic as it has a lower earning rate. The BE traffic is followed by Class B and then Class A. In some cases Class B might have a higher percentage of carried traffic. This is because of the approximation to the LP-to-INT approach, network topology and VPN distribution. The result is shown for both LP and LP-to-INT approach. The average hop number also starts to drop as the demand increases. This is because the route with a larger hop number utilizes more resources and this is undesirable when resources are deficient. In Figures 2.14-2.20 we show the effect of one stage routing for Networks 1, 2 and 3.

In two stage routing, the QoS and BE traffic are routed separately in two different stages. In the first stage, the high priority QoS traffic is routed allowing it to use the available link capacities. In the second stage, the BE traffic is routed and it uses the residual capacities left after routing QoS traffic. Our results show that in this method of routing, BE has a higher percentage of carried traffic than in onestage routing. The result is shown for both LP and LP-to-INT approach. The average hop number also starts to drop as the demand increases. This reduces the resource utilization when resources are deficient and helps in maintaining the network revenue. In Figures 2.21-2.27 we show the effect of two stage routing for Networks 1, 2 and 3. It is clearly seen that the percentage of carried traffic for BE is higher than that in onestage routing.

- **Effect of Hop Constraint**

In this section we show the performance of QoS traffic under the hop constraint. The hop constraint is set only for Class A and Class B traffic of all VPN's. BE traffic is unaffected by the hop constraint. We consider two different sets of traffic demands : a light load and a heavy load, to show the effect of the hop constraint. The light load has less demands and is sufficient to carry all the VPN traffic in the network. The heavy load is more than the network can afford, and results in the dropping of demands for certain VPNs. The Figure 2.28, show the performance of each network under light load conditions. We observe that once the hop bound is more then the maximum number of hops, the network acts as if no hop constraint is imposed. At a lower value of the hop number, the percentage of carried traffic for Class A and Class B is low and as the hop number increases the amount of carried traffic also increases. Beyond the maximum hop number, the hop constraint does not have any effect. Also, we observe that the BE traffic is not affected by the hop constraint.

In Figure 2.29, we show the performance of the network under heavy load conditions. In this case we observe that all of the BE traffic is not allocated bandwidth. This is because of the heavy load conditions. When the hop bound is less, the percentage of carried traffic for Class A and Class B is less. But, as the hop bound increases, the network can accommodate more of class A and class B traffic and BE traffic is dropped due to the heavy load.

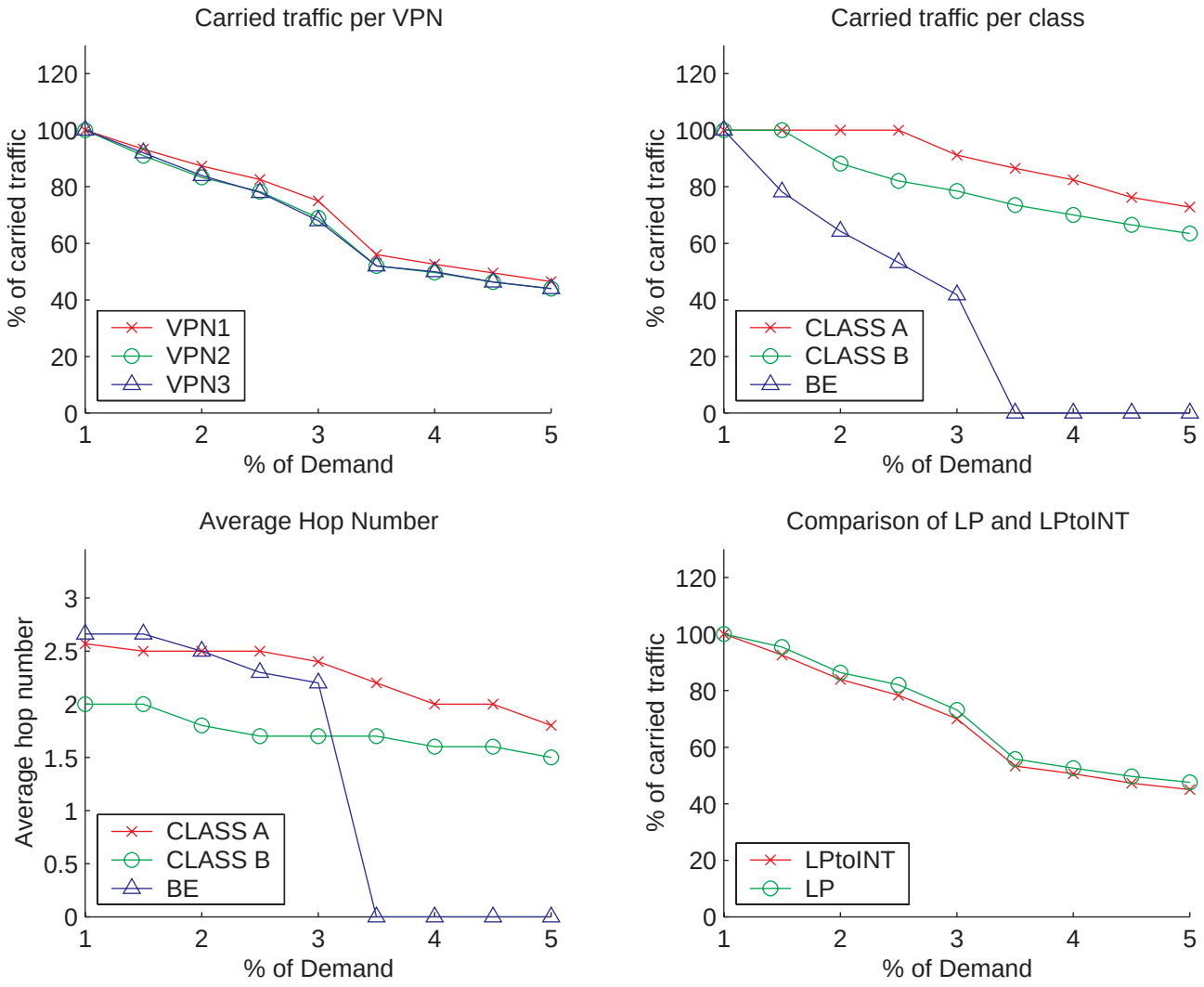

Figure 2.14: Effect of e_{s,σ^t} for Network 1: One Stage Routing

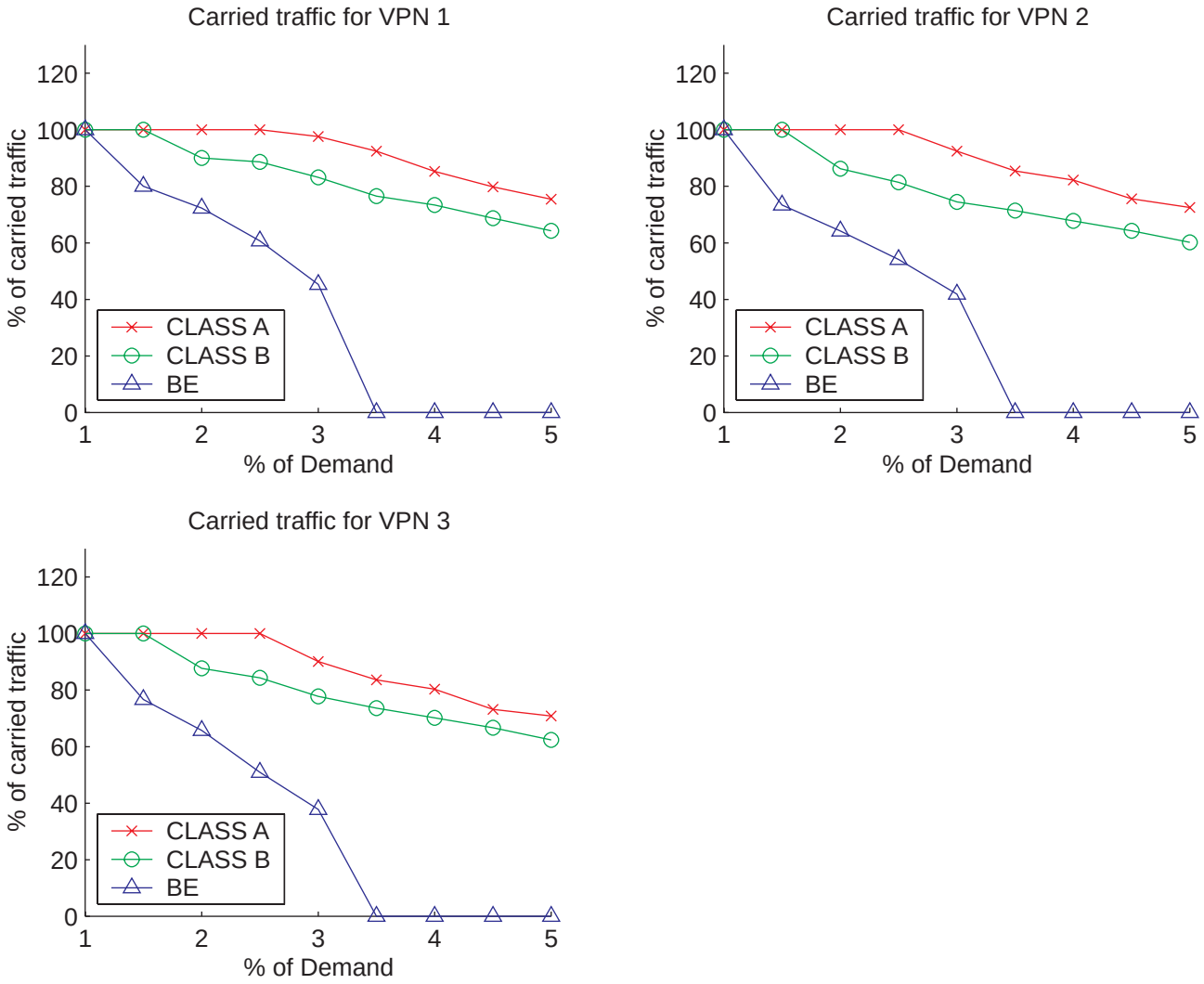

Figure 2.15: Effect of e_{s,σ^t} for Network 1: One Stage Routing

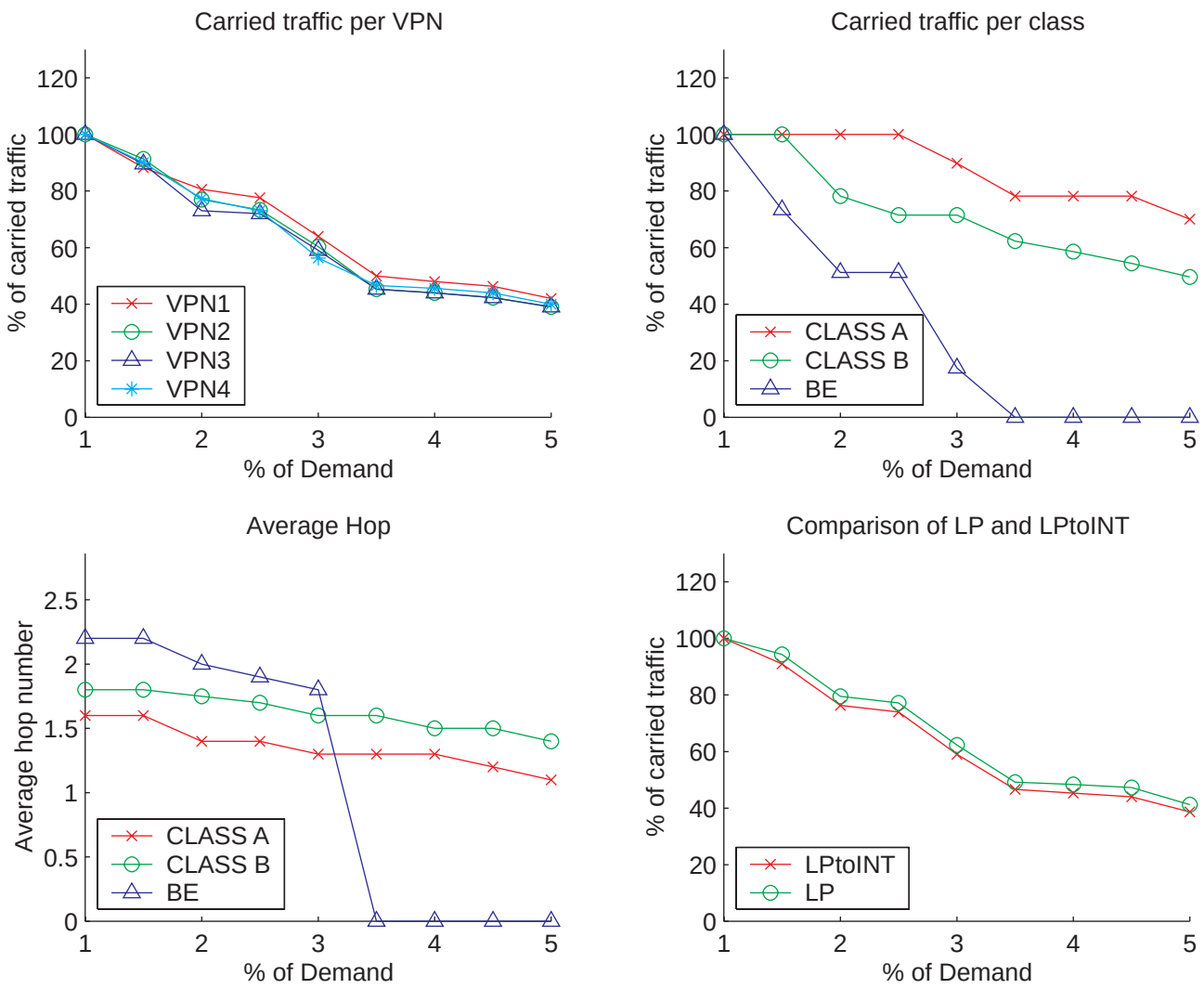

Figure 2.16: Effect of e_{s,σ^t} for Network 2: One Stage Routing

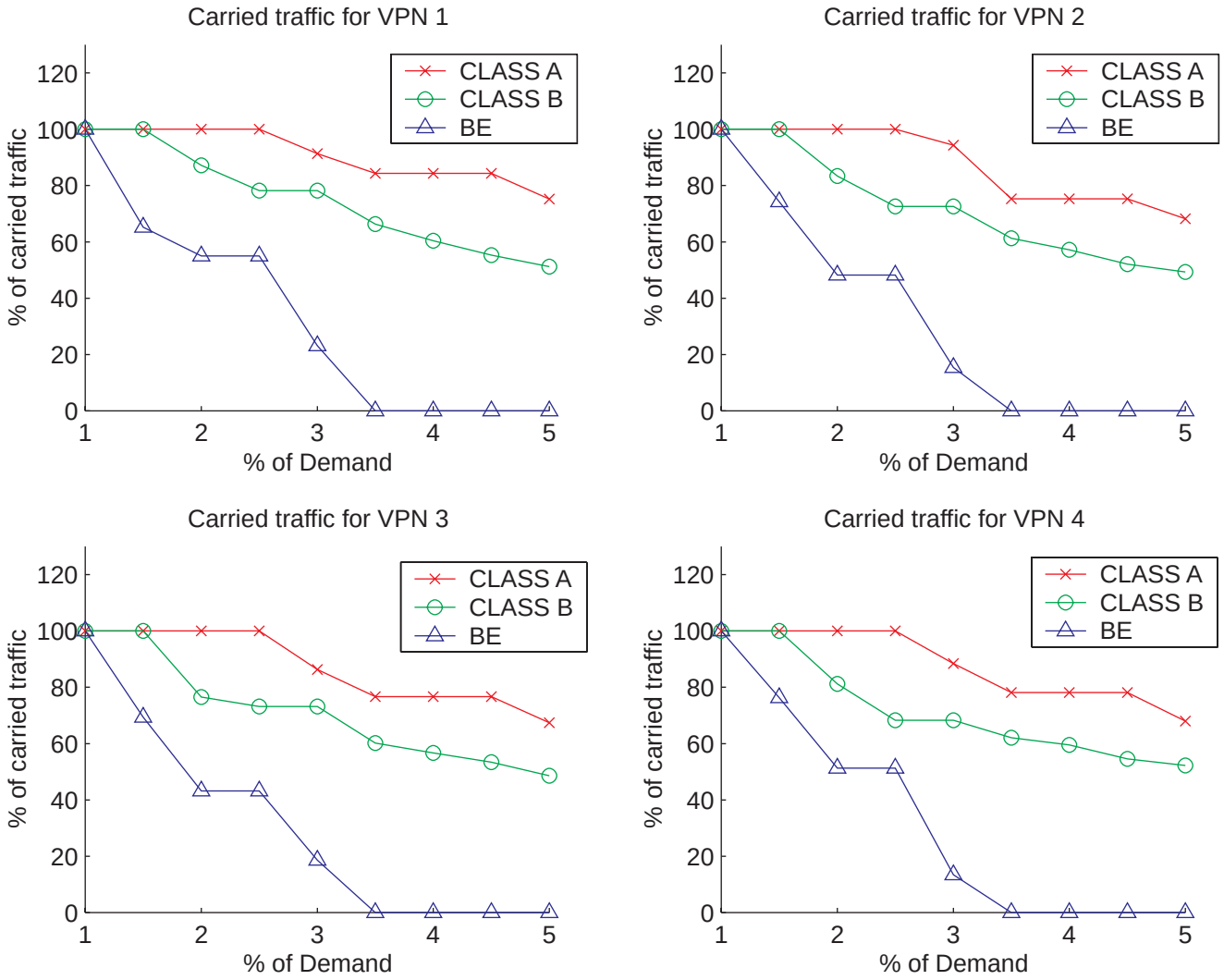

Figure 2.17: Effect of e_{s,σ^t} for Network 2: One Stage Routing

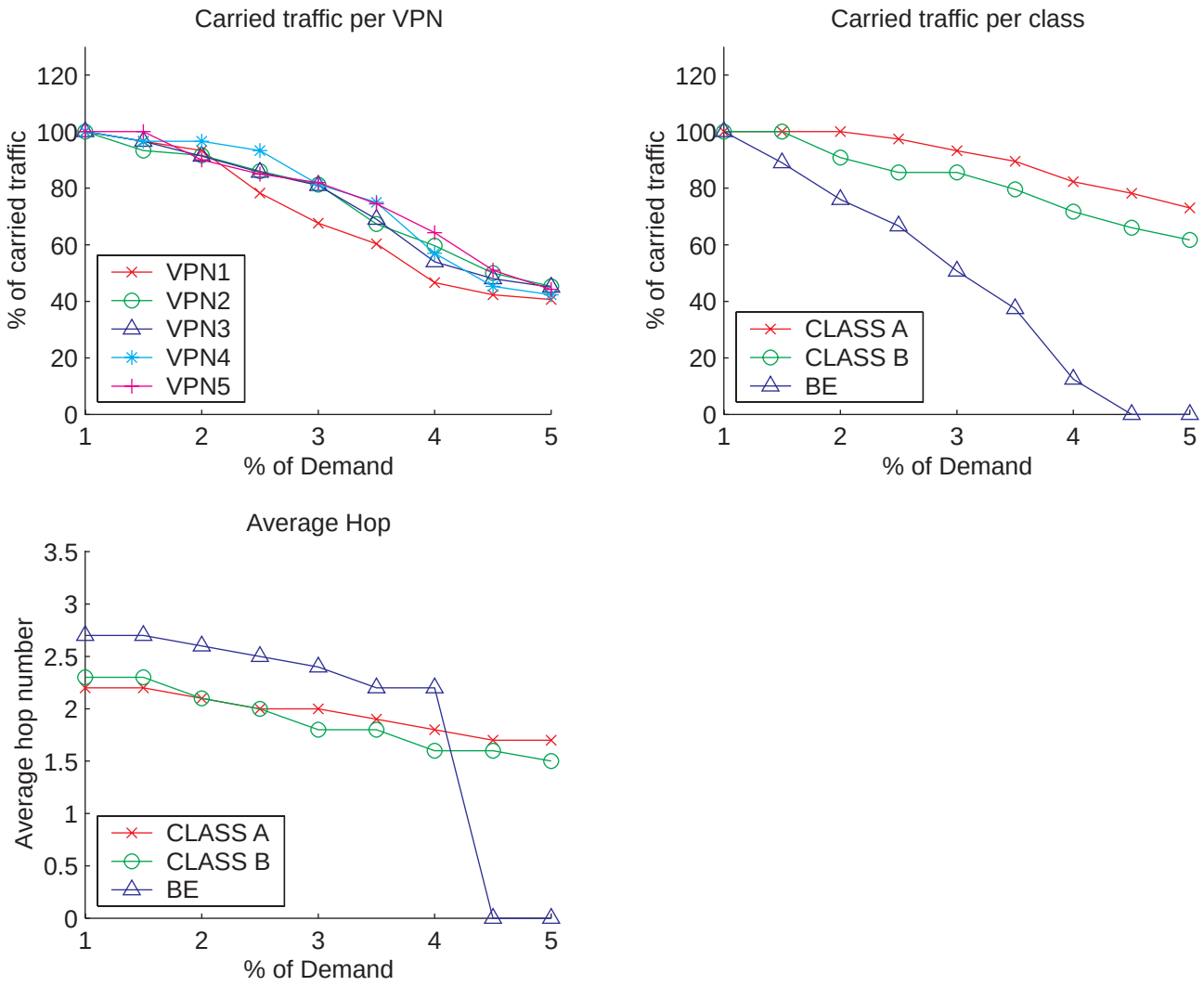

Figure 2.18: Effect of e_{s,σ^t} for Network 3: One Stage Routing

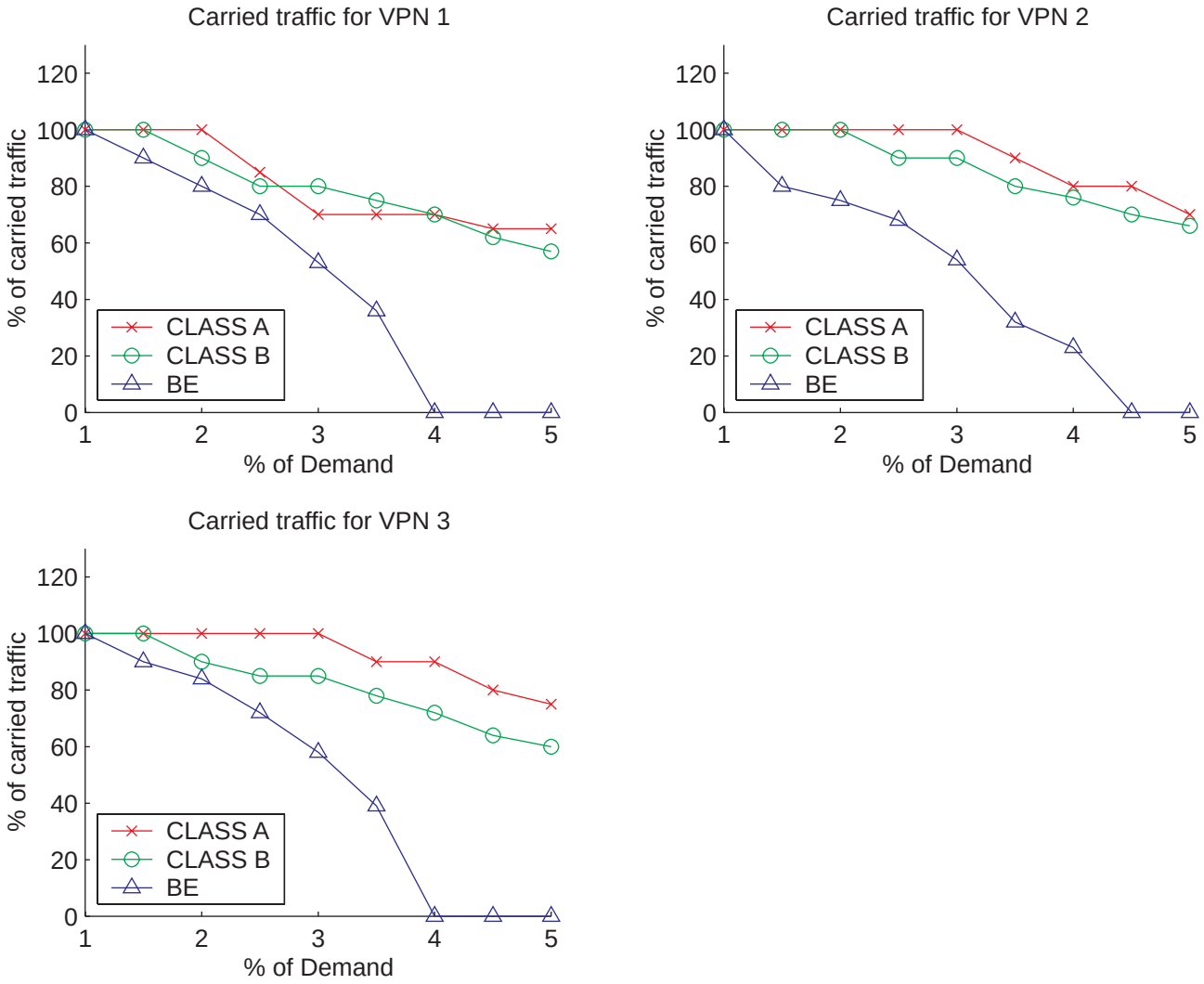

Figure 2.19: Effect of e_{s,σ^t} for Network 3: One Stage Routing

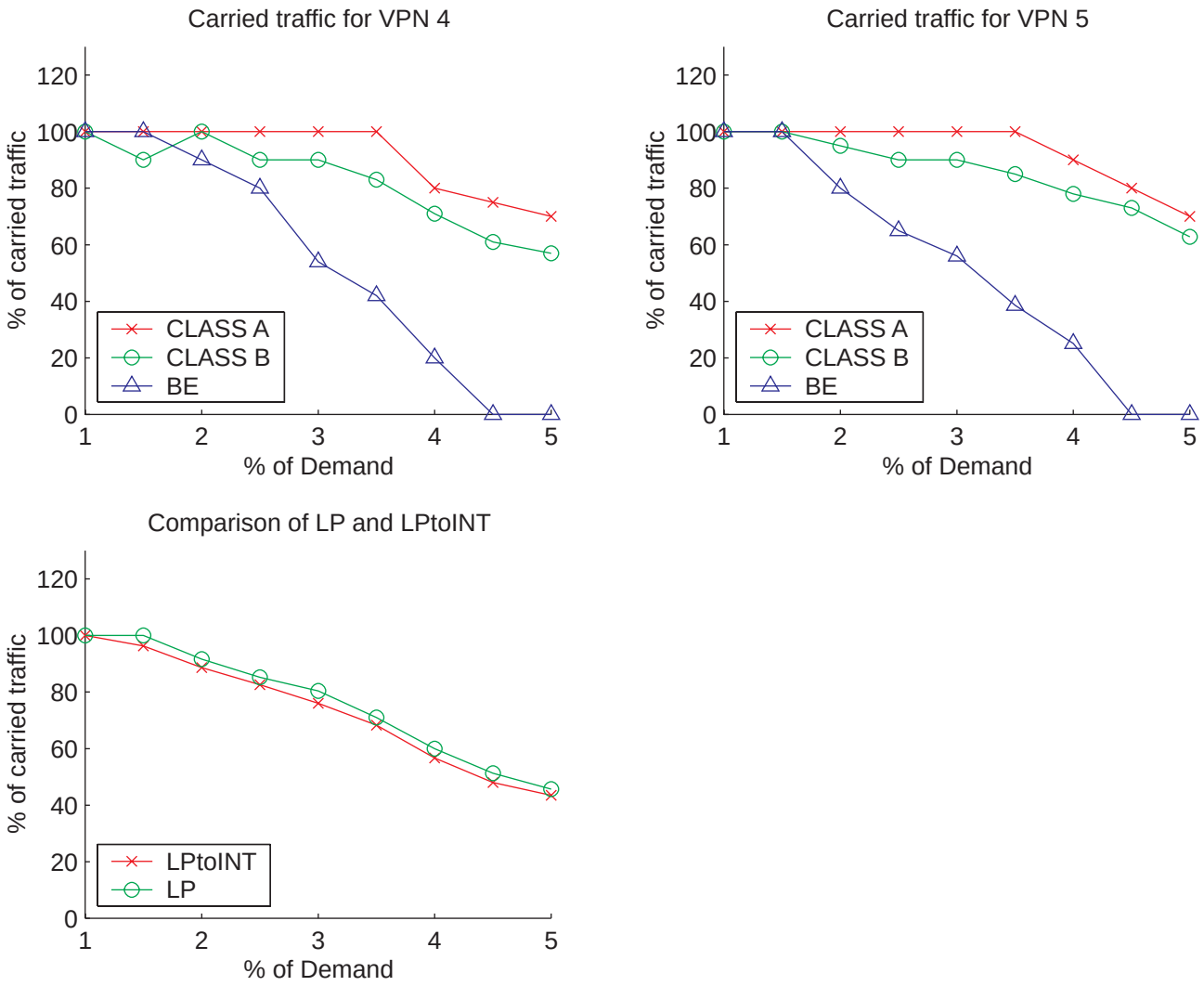

Figure 2.20: Effect of e_{s,σ^t} for Network 3: One Stage Routing

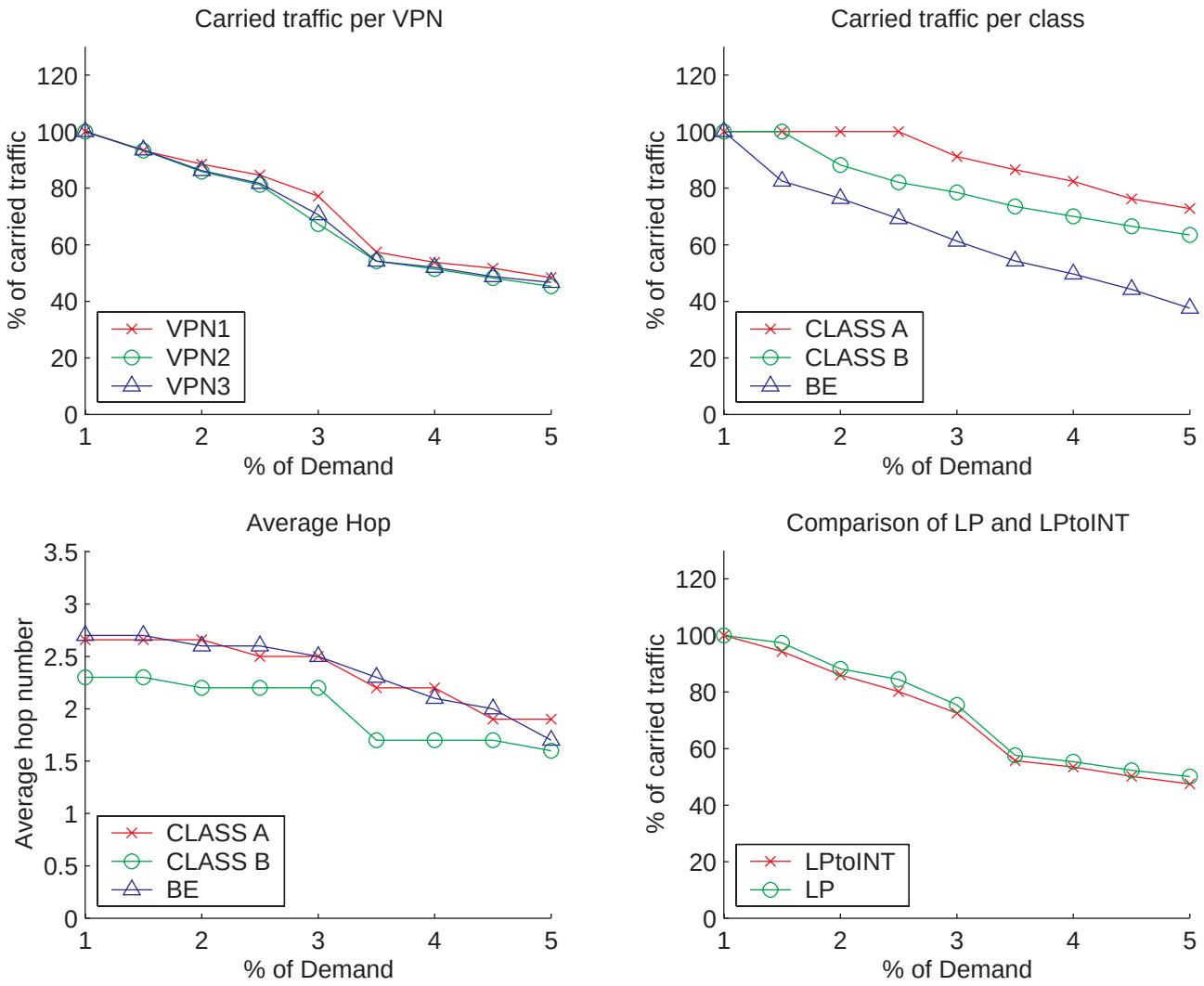

Figure 2.21: Effect of e_{s,σ^t} for Network 1: Two Stage Routing

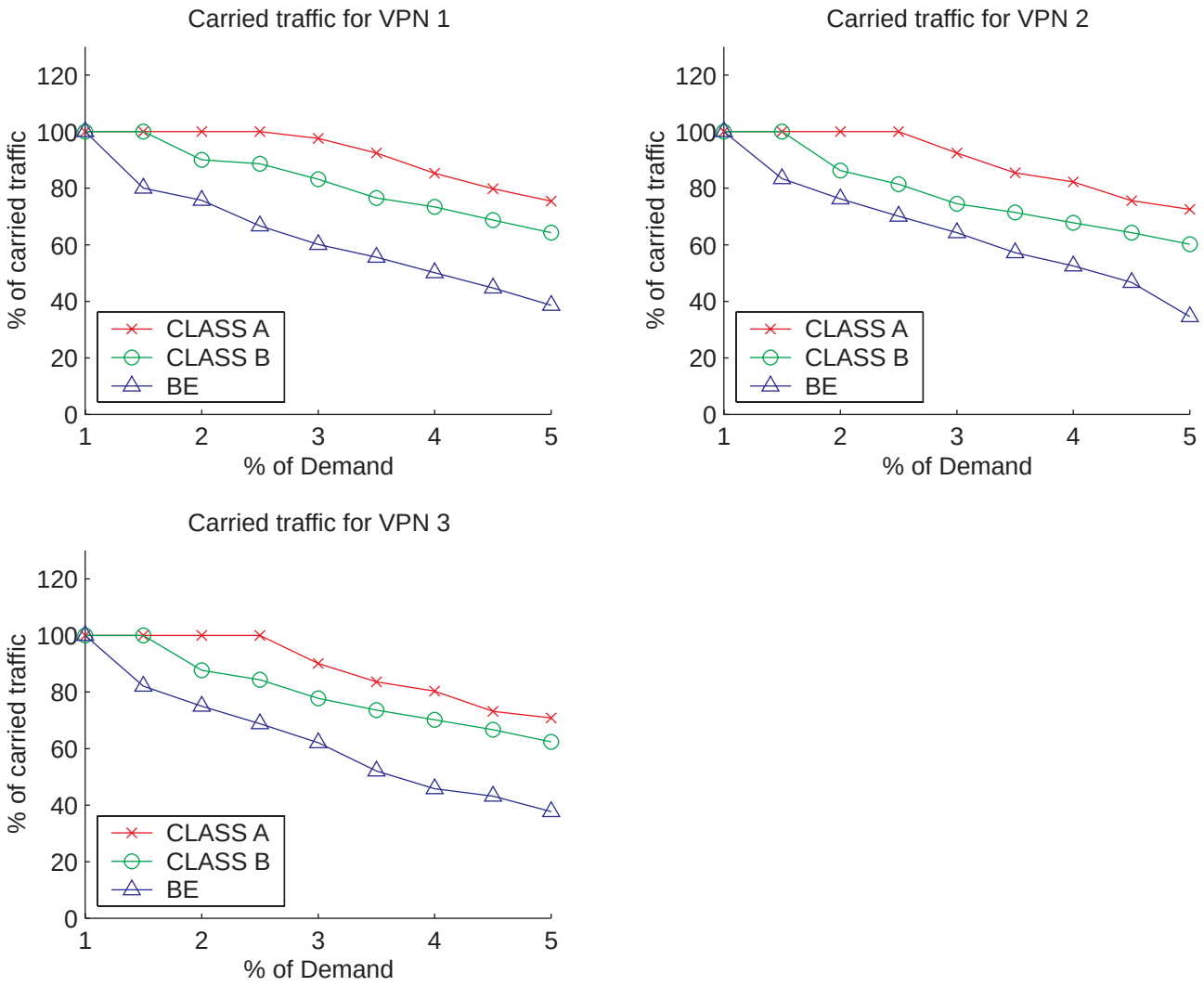

Figure 2.22: Effect of e_{s,σ^t} for Network 1: Two Stage Routing

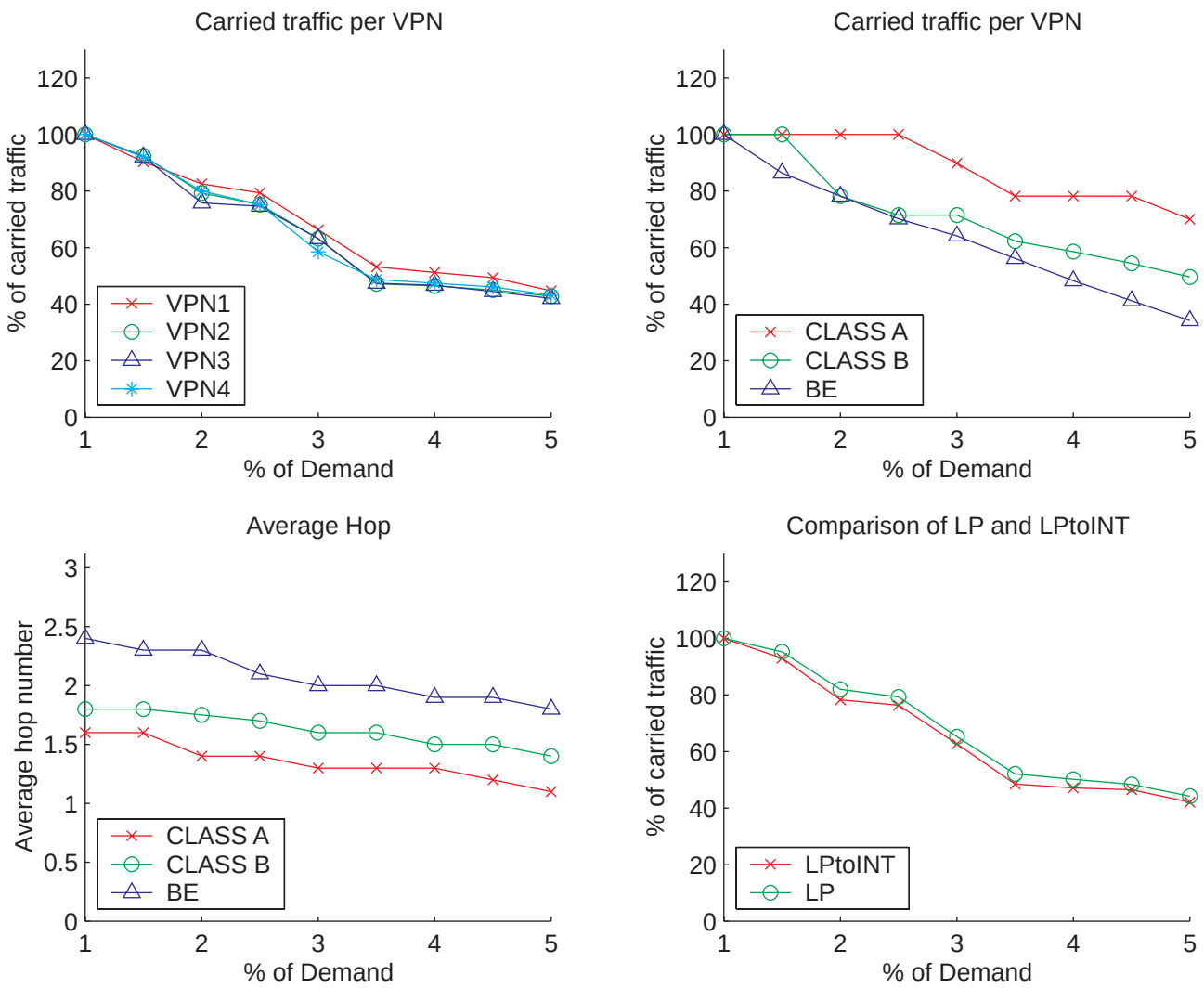

Figure 2.23: Effect of e_{s,σ^t} for Network 2: Two Stage Routing

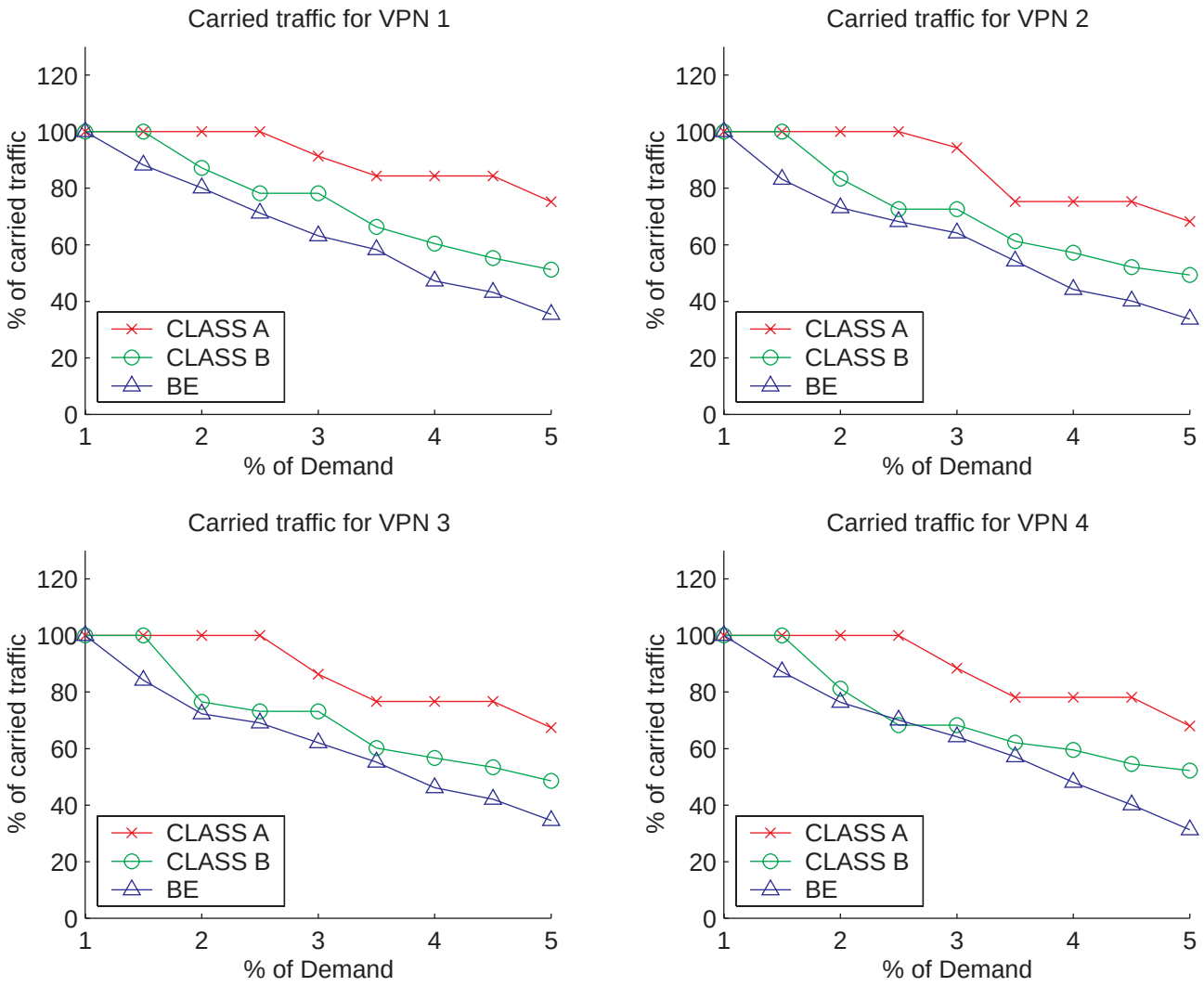

Figure 2.24: Effect of e_{s,σ^t} for Network 2: Two Stage Routing

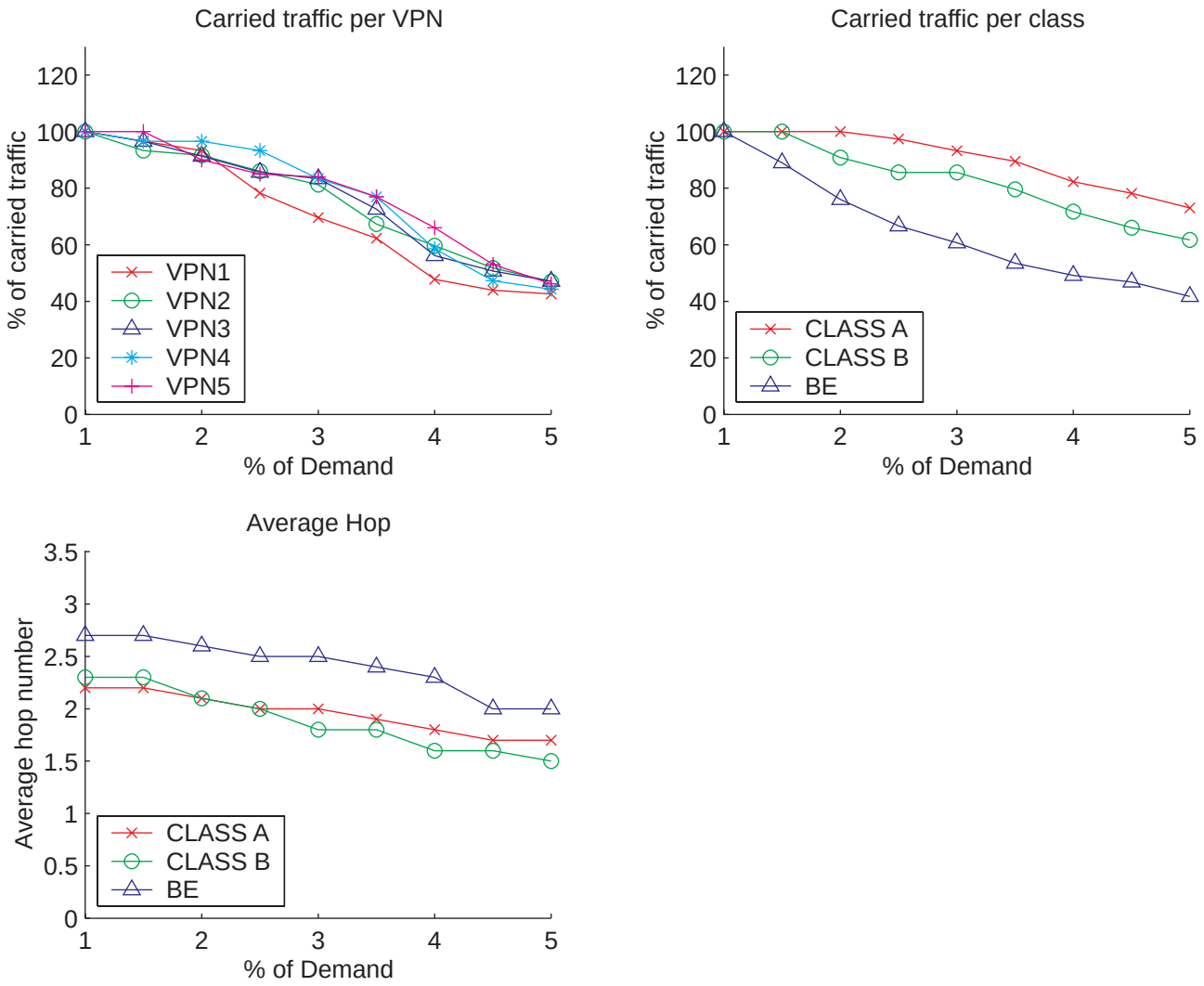

Figure 2.25: Effect of e_{s,σ^t} for Network 3: Two Stage Routing

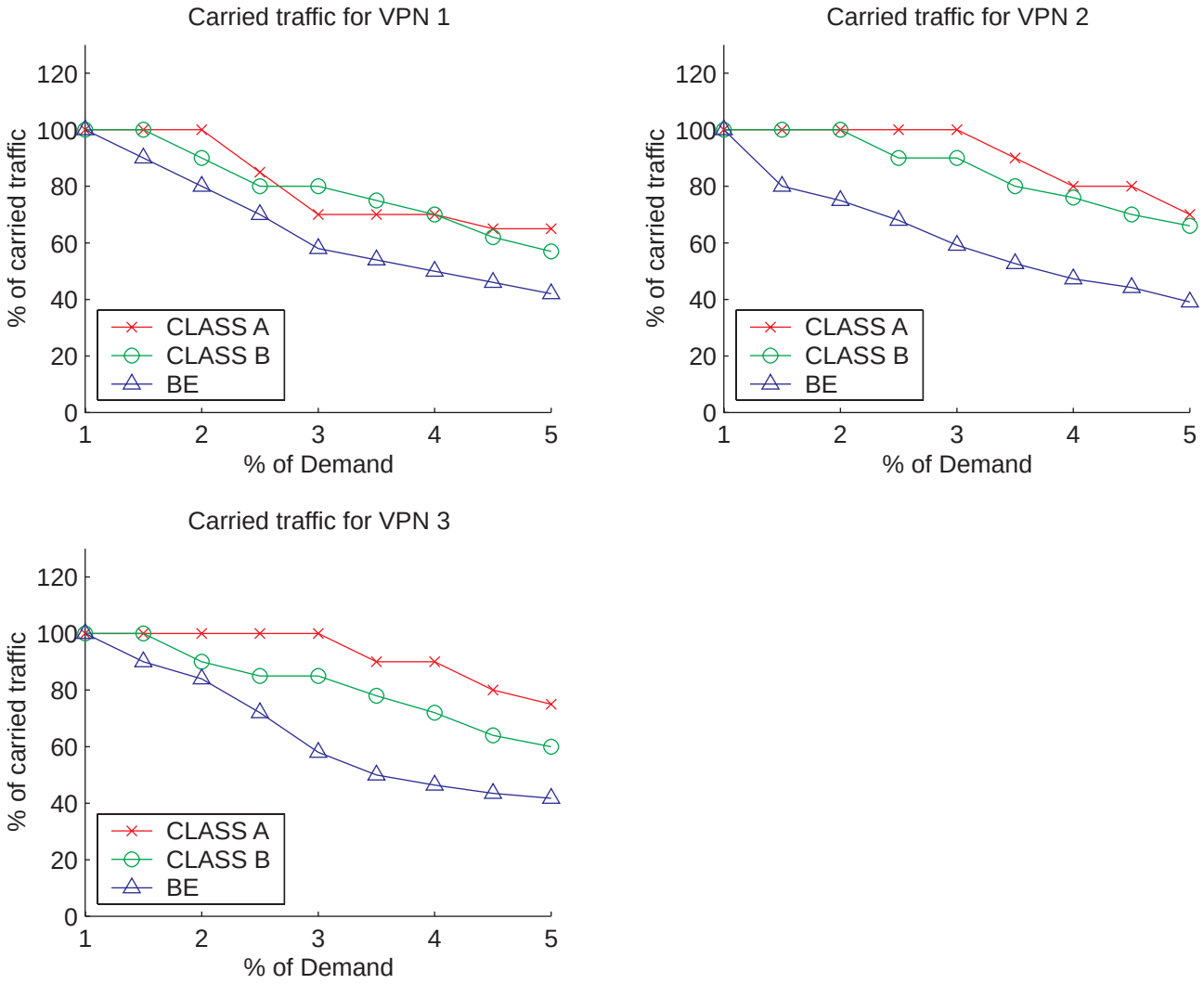

Figure 2.26: Effect of e_{s,σ^t} for Network 3: Two Stage Routing

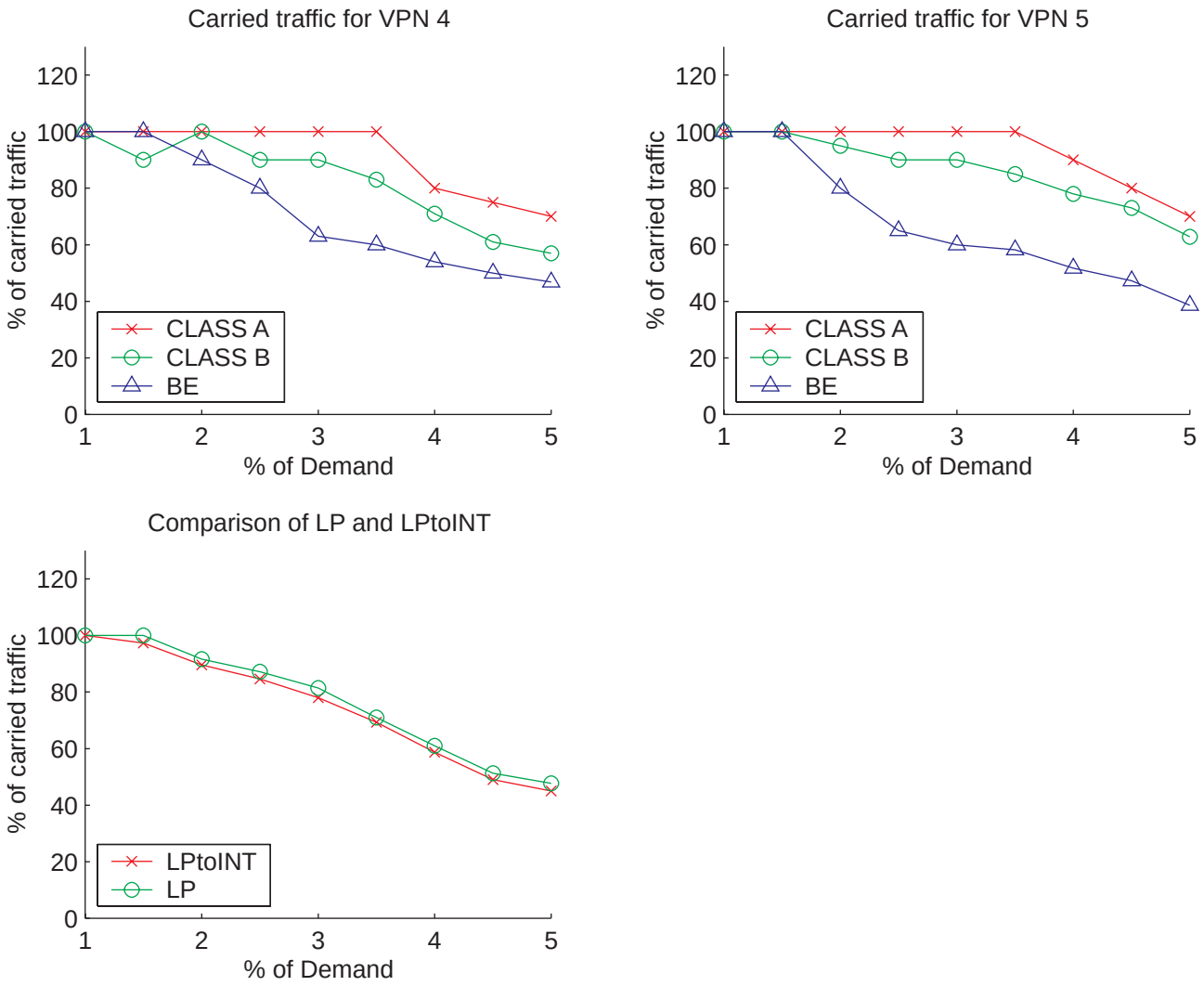

Figure 2.27: Effect of e_{s,σ^t} for Network 3: Two Stage Routing

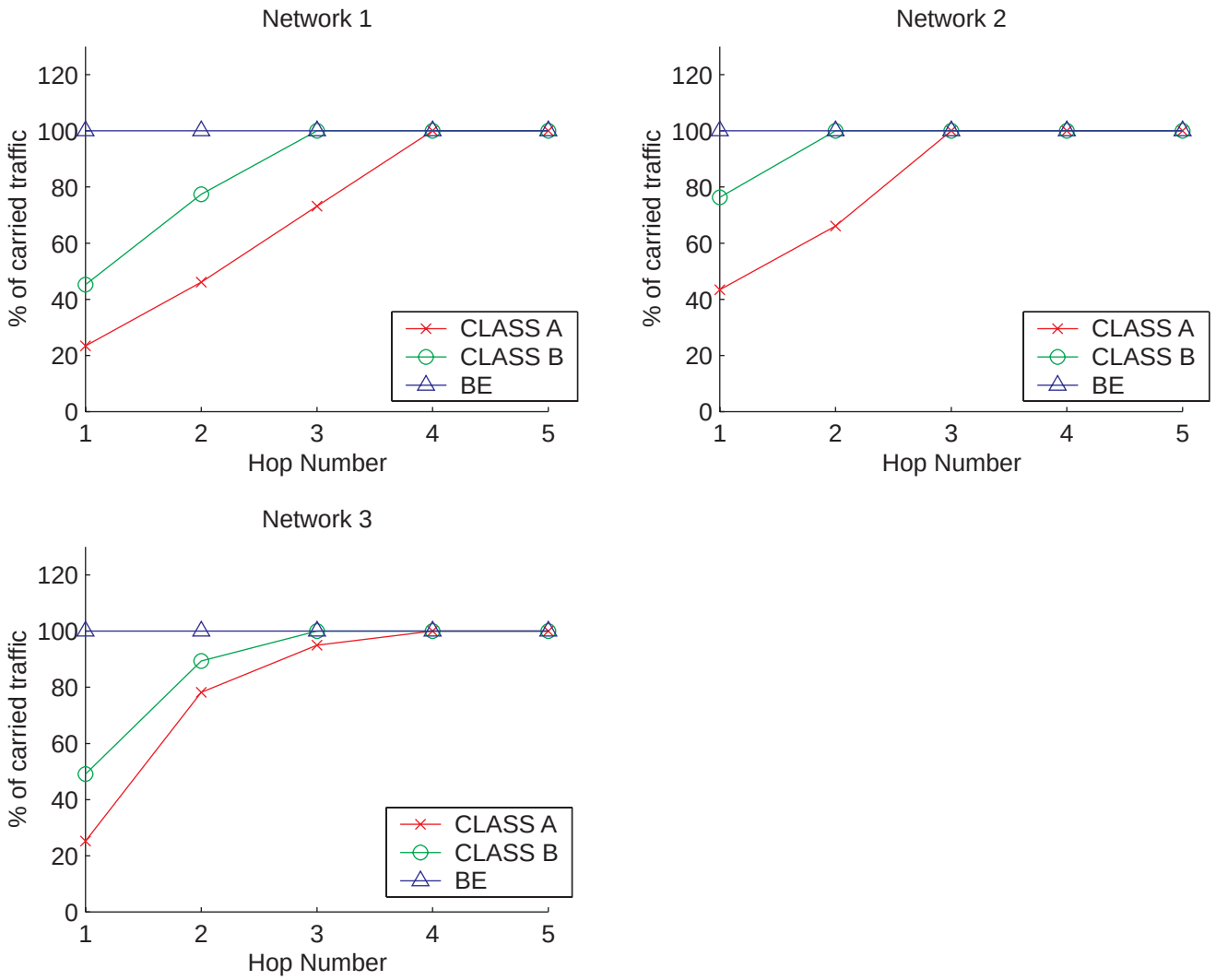

Figure 2.28: Effect of hop constraint under light load

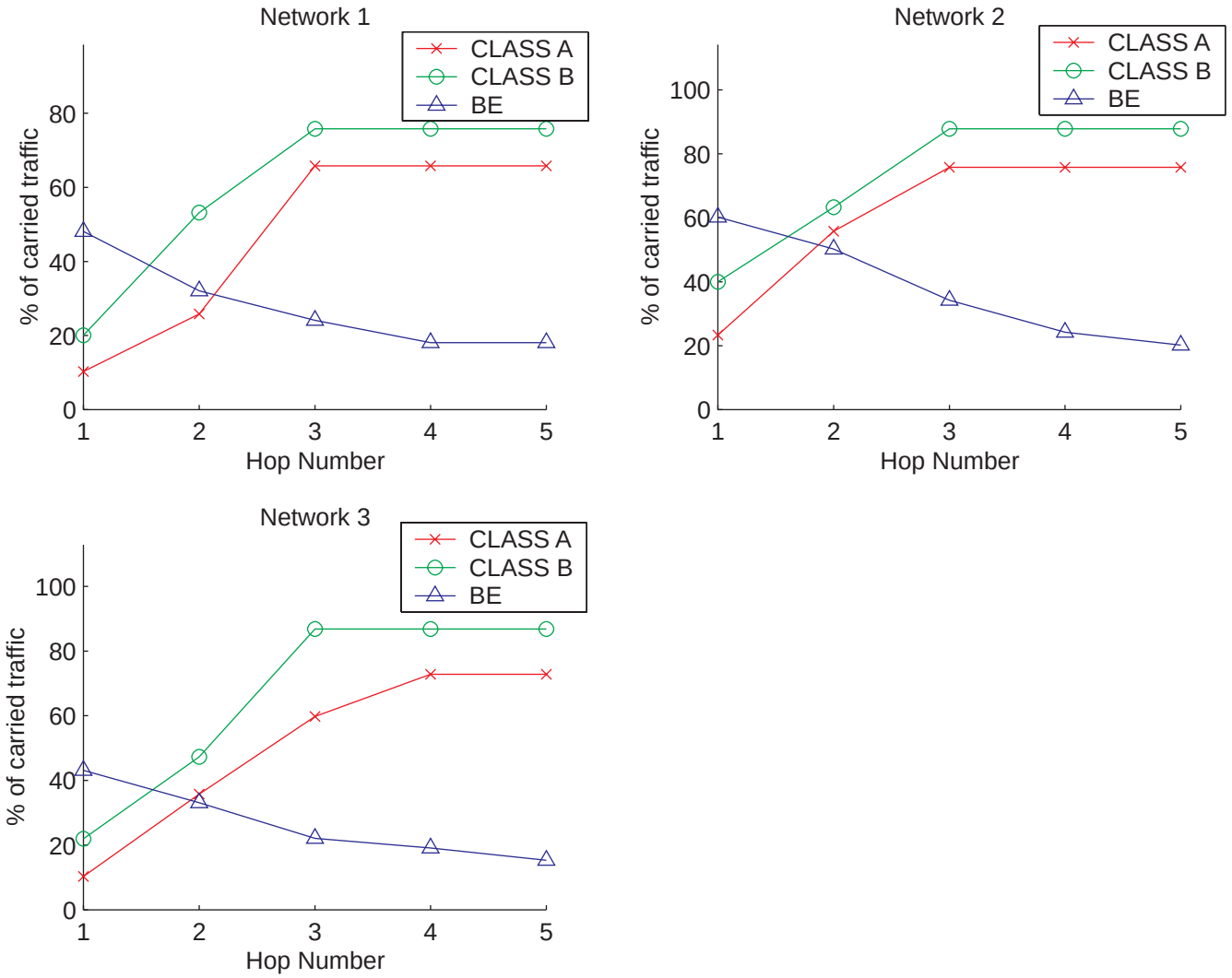

Figure 2.29: Effect of hop constraint under heavy load

Chapter 3

Path Protection

3.1 Introduction

In this chapter we introduce the path protection algorithms for MPLS Virtual Private Networks.In section (3.2) we review the path protection techniques proposed in [4]. Our approach to path protection in MPLS Virtual Private Networks is introduced in section (3.3). The experimental results for our approach is explained in section (3.4).

3.2 Previous Work

In [4], the authors proposed both $1 + 1$ and $1 : 1$ link and node disjoint path protection schemes for an MPLS network.In section 3.2 we explain the method of establishing the backup paths as in [4] and provide the constraints for link disjoint and node disjoint backup. The length of the backup path is important for effective traffic engineering and this is explained in section 3.2.

Path Protection schemes

Path protection in the network is provided only for the QoS class of traffic. The establishment of the backup path is very similar to that of a primary path. Backup paths are established based on MCF problem P7 for different classes of QoS traffic and OD pairs depending on the kind of service requested. Path protection can be link-disjoint where , none of the links $l \in L$ in the network are shared by the primary and backup paths for a given OD pair and a given class s. This is to ensure that failure of a certain link on the primary path will not affect the backup path. In node-disjoint path protection the primary and backup paths for a given OD pair and a given class s do not share a common node. This ensures that failure of a node in the primary path will not affect the traffic flow in the backup path. The 1+1 path protection requires two link-disjoint or two node-disjoint label switched paths for a single OD pair. In this scheme all classes of traffic is routed in a single stage. The 1:1 path protection scheme requires that the resources of the backup path are available to preemptible low priority traffic. In this mechanism the traffic is routed in two

different stages. In the first stage the high priority QoS traffic is routed and in the second stage the low priority Best Effort traffic is routed which uses the residual capacities.

The backup path can be easily created as a new OD pair.Thus there is an additional OD pair from the same source node to the same destination node. Let σ_p be the OD pair for QoS traffic on the primary or the working path and σ_b be the OD pair for the backup path. Since the OD pairs for both the primary and backup paths are the same, they will have the same demand i.e $D_{\sigma_p} = D_{\sigma_b}$. We let $F_{\sigma_p} = F_{\sigma_b}$ so the bandwidth allocated on the primary and the backup paths are the same. As a result, the traffic on both the paths will be accepted or rejected simultaneously.

The backup path can be link disjoint or node disjoint with the primary path. The granularity g is set to 1 to prevent splitting of traffic along multiple LSP's. Hence, there is a single LSP established for each traffic demand. The link-disjoint constraint given in [4] is given below:

$$Y_{\sigma_p,l} + Y_{\sigma_b,l} \leq D_{\sigma_p}, \forall l. \tag{3.1}$$

The constraint (3.1), ensures that the link l is utilized either by the primary path or the backup path, and not both.

The node disjoint constraint for the primary path and backup path proposed in [4] is as follows.

$$\sum_{l \in L_i(n)} Y_{\sigma_p,l} + \sum_{l \in L_i(n)} Y_{\sigma_b,l} \leq D_{\sigma_p}, \forall n \notin T, \tag{3.2}$$

or

$$\sum_{l \in L_o(n)} Y_{\sigma_p,l} + \sum_{l \in L_o(n)} Y_{\sigma_b,l} \leq D_{\sigma_p}, \forall n \notin S. \tag{3.3}$$

The constraint (3.2) ensures that either the primary path OD pair σ_p or the backup path OD pair σ_b has the traffic entering node n. Similarly (3.3) ensures that either the OD pair σ_p or the OD pair σ_b has the traffic leaving node n. T is the set of all source nodes in the network and S is the set of all destination nodes in the network. The above constraints hold good only when the problem is a non-bifurcation problem.

Length of the Backup Path

While establishing the primary and backup paths, it is possible that the backup path established might be shorter than the primary path. This is undesirable as it prevents efficient traffic engineering. The longer working path will use more resources and cause more delay while there is a shorter available path. The hop constraint discussed earlier ensures that the primary and the backup path will have a limited hop count, but a longer path could still be chosen for the primary path. To prevent this situation, we need to distinguish between the primary and backup paths. Since the longer path uses more network resources, a parameter B_σ is introduced to distinguish the utilized resources between the working path and the backup path The MCF problem with the parameter B_σ as given in [4] is as follows.

$$maximize \quad \sum_{\sigma} e_{s,\sigma} F^s_\sigma - \varepsilon \sum_{\sigma} B_\sigma \sum_{l} Y_{\sigma,l}. \tag{3.4}$$

B_σ is used to differentiate the working path and backup path. The parameter B_σ is chosen to be larger for the primary path than the backup path. Thus, in (3.4), if a working path utilize more resources than backup path, we will obtain less revenue. Since our objective is to maximize the revenue, this situation will not happen, and we can obtain a shorter working path.

3.3 Our Approach to Path Protection in MPLS VPN's

The approach discussed in section(3.2) hold good for a single MPLS network. We have extended this approach to accommodate MPLS Virtual Private Networks.

3.3.1 Path Protection in MPLS VPN's

Path protection is provided depending on the service requested. The technique of establishing backup paths is similar to that presented in section [3.2.1]. In the $1+1$ path protection scheme, the primary and the backup path resources are reserved for the high priority QoS traffic. There is no sharing of the backup path resources. The backup path carries a second copy of the traffic on the primary path. The traffic in this method is routed in a single stage. $1+1$ path protection can be either link disjoint or node disjoint. In $1:1$ path protection, the traffic is routed in two separate stages. In the first stage, only the high priority QoS traffic is routed allowing it use all available link capacities. In the second stage, the low priority Best Effort traffic is routed which uses the residual capacities on all the links. In this method, there is a sharing of backup path resources. $1+1$ path protection can be implemented as either link disjoint or node disjoint. The notations uses in our approach are given in Table 3.1.

The link disjoint constraint for our approach is as follows:

$$Y^l_{s,\sigma^t_p} + Y^l_{s,\sigma^t_b} \leq D_{s,\sigma^t_p}, \quad \forall l \tag{3.5}$$

The constraint (3.5) ensures that the link l is only utilized by the primary path or the backup path and not both.

The node disjoint constraint for our approach is as follows:

$$\sum_{l \in L_i(n)} Y^l_{s,\sigma^t_p} + \sum_{l \in L_i(n)} Y^l_{s,\sigma^t_b} \leq D_{s,\sigma^t_p}, \quad \forall n \notin T \tag{3.6}$$

or

$$\sum_{l \in L_o(n)} Y^l_{s,\sigma^t_p} + \sum_{l \in L_o(n)} Y^l_{s,\sigma^t_b} \leq D_{s,\sigma^t_p}, \quad \forall n \notin S \tag{3.7}$$

(3.6) ensures that the traffic entering node n is either on the OD pair σ^t_p or on the OD pair σ^t_b. (3.7) ensures that the traffic leaving node n is either on the OD pair σ^t_p or on the

Table 3.1: Notation of MCF problem for Path Protection of QoS traffic.

σ_p^t	Origin Destination pair for vpn t on the primary path
σ_b^t	Origin Destination pair for vpn t on the backup path
C_l	Capacity on link l
B_σ	parameter for backup path
D_{s,σ_p^t}	Bandwidth demand for class s and OD pair σ for VPN t for the primary path
D_{s,σ_b^t}	Bandwidth demand for class s and OD pair σ for for VPN t the backup path
S_{QoS}	The set of service classes for QoS traffic
W_{QoS}	network revenue for QoS traffic
F_{s,σ_p^t}	Carried bandwidth for class s,OD pair σ_p and VPN t on the primary path
F_{s,σ_b^t}	Carried bandwidth for class s,OD pair σ_p and VPN t on the backup path
Y^l_{s,σ_p^t}	Carried bandwidth for class s,OD pair σ_p and VPN t on the primary path
Y^l_{s,σ_b^t}	Carried bandwidth for class s,OD pair σ_p and VPN t on the backup path

OD pair σ_b^t. The above link and node disjoint constraints hold good only for the traffic non-bifurcation case when granularity g is set to one.

To ensure that a shorter path is chosen for the primary path and to distinguish between the primary and backup paths , the objective function is modified to include the backup parameter B_σ discussed in section 3.2. The objective function in the MCF problem $P10$ along with the backup path parameter B_σ is as follows: *MCF Problem P10:*

$$Maximize \;\; W_{QoS} = \sum_s \sum_t \sum_\sigma e_{s,\sigma^t} F_{s,\sigma^t} - \epsilon \sum_s \sum_t \sum_\sigma B_\sigma \sum_l Y^l_{s,\sigma^t} \tag{3.8}$$

The parameter B_σ (3.8) ensures that a shorter path is chosen for the primary path than the backup path.

3.4 Experimental Results

In this section we present the experimental results for $1+1$ and $1:1$ link disjoint and node disjoint path protection mechanisms. The graphs verify the efficiency of the path

protection scheme for different cases including the sharing of the backup resources, the link-disjoint constraint, the node-disjoint constraint and the use of B_σ. In Section 3.4.1, the networks used and the experimental configuration is described. In Section **??**, the result of the experiments are illustrated and discussed.

3.4.1 Simulation Configuration

The network models used are similar to that of QoS traffic in Section 2.4.1. We have two high priority QoS classes Class A and Class B and the low priority Best Effort traffic. Backup paths are established only for the QoS classes of traffic. The bandwidth is assigned for the traffic demand between a OD pair only when both the primary path and backup path can be accommodated for that OD pair.

We compare the performance of $1+1$ and $1:1$ path protection scheme. In $1+1$ path protection, the backup resources of the QoS traffic are not shared by the BE traffic, the resources of the backup paths are fully occupied by another copy of the carried traffic. In the $1:1$ path protection, the resources of the backup path are available to the BE traffic. There is a sharing of resources between the QoS and the BE traffic classes. The resource of backup paths are considered as the residual capacities available for the BE traffic. B_σ has to be chosen carefully to make sure it does not affect the use of ε. B_σ is intended to reduce the importance of resources reserved for backup path comparing to the resources allocated for the primary path. Therefore, B_σ is assigned a smaller value in the backup path than in the primary path. In our experiments, we set $B_\sigma = 1$ for the working path and $B_\sigma = 0.1$ for the backup paths.

3.4.2 $1+1$ and $1:1$ Path Protection

In this section, we show the experimental results and performance of each of the backup schemes. We also show the effect of the parameter B_σ in $1+1$ and $1:1$ path protection mechanism. We explain the results for the $1+1$ path protection mechanism and $1:1$ path protection mechanism in the sections that follow. The results for both link and node disjoint path protection mechanisms is shown.

- $1+1$ **Link Disjoint Path Protection**

In Figures 3.1 - 3.2 we show the results of $1+1$ link-disjoint path protection scheme with B_σ for network 1.In Figures 3.4 - 3.6 we show the results of $1+1$ link-disjoint path

protection scheme with B_σ for network 2. In Figures 3.8 - 3.10 we show the results of $1+1$ link-disjoint path protection scheme with B_σ for network 3.

The percentage of carried traffic, average hop number and backup average hop number are plotted vs the percentage of demand. The percentage of carried traffic for each class of each VPN is also shown. The results are shown both for LP and LP-to-INT. The LPI solution shows the round off effect with the increase in demand. As the traffic demand increases, the percentage of traffic carried drops.

The difference from the QoS traffic experiment using two stage routing is that all classes of traffic drops early because of the demand of the backup path.The BE traffic is dropped first due to its lower priority followed by the other QoS classes. early because of the backup provided to class A and class B. It is seen that the average backup hop number is larger compared the average hop number of working path. This shows that a longer path is selected for the backup path.It is also seen that as the demand increases the average hop number also drops. This is done to conserve resources as a longer path would utilize more resources.

We also show the link-disjoint path protection scheme without differentiation between the working path and backup path i.e without the parameter B_σ in 3.3, 3.7 and 3.11 for networks 1,2 and 3. We observe from the graphs that the average backup hop number is smaller compared to the average hop number of working path showing the effect of B_σ.

- $1+1$ **Node Disjoint Path Protection**

In Figures 3.12 - 3.13 we show the results of $1+1$ node-disjoint path protection scheme with B_σ for network 1. In Figures 3.15 - 3.17 we show the results of $1+1$ node-disjoint path protection scheme with B_σ for network 2. In Figures 3.19 - 3.21 we show the results of $1+1$ node-disjoint path protection scheme with B_σ for network 3.The percentage of carried traffic, average hop number and backup average hop number are plotted vs the percentage of demand. The results are shown both for LP and LP-to-INT. The results are similar to link disjoint backup scheme except that the QoS traffic of each VPN is dropped earlier. This is because it is difficult to establish a node disjoint backup path when compared to a link disjoint backup path. We see that the average hop number also drops as the demand increases as in the link protection scheme. The effect of the parameter B_σ is also seen.

In Figures 3.14, 3.18 and 3.22 we show the $1+1$ node-disjoint path protection scheme without differentiation between the working path and backup path i.e without the parameter B_σ. We observe from the graphs that the average backup hop number is smaller compared the average hop number of working path showing the effect of B_σ that a shorter path is chosen for the backup path in the absence of B_σ. The percentage of carried traffic drops as the demand increases and is faster than the drop in case of the link disjoint backup.

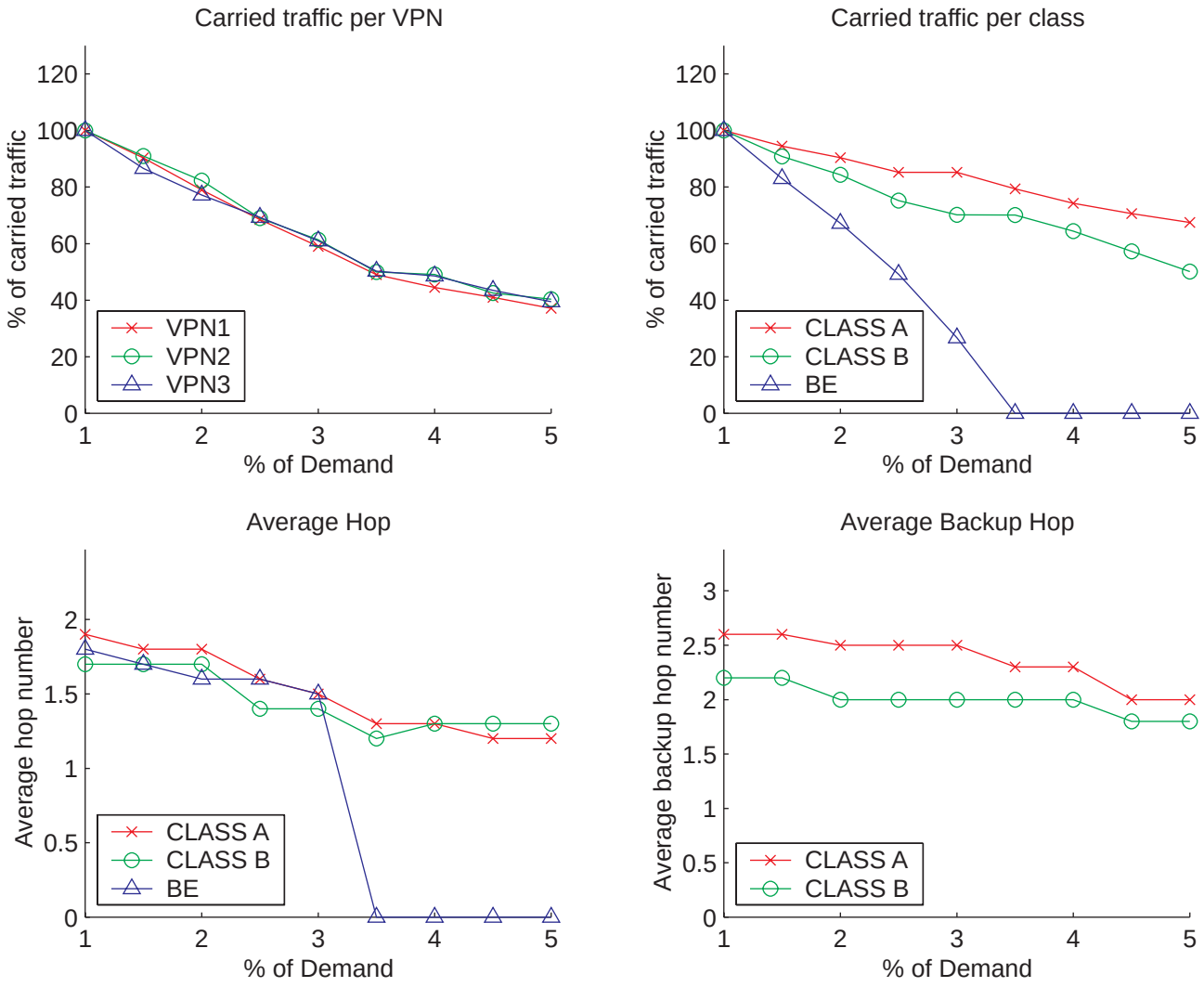

Figure 3.1: 1+1 link disjoint path protection with B_σ for Network 1

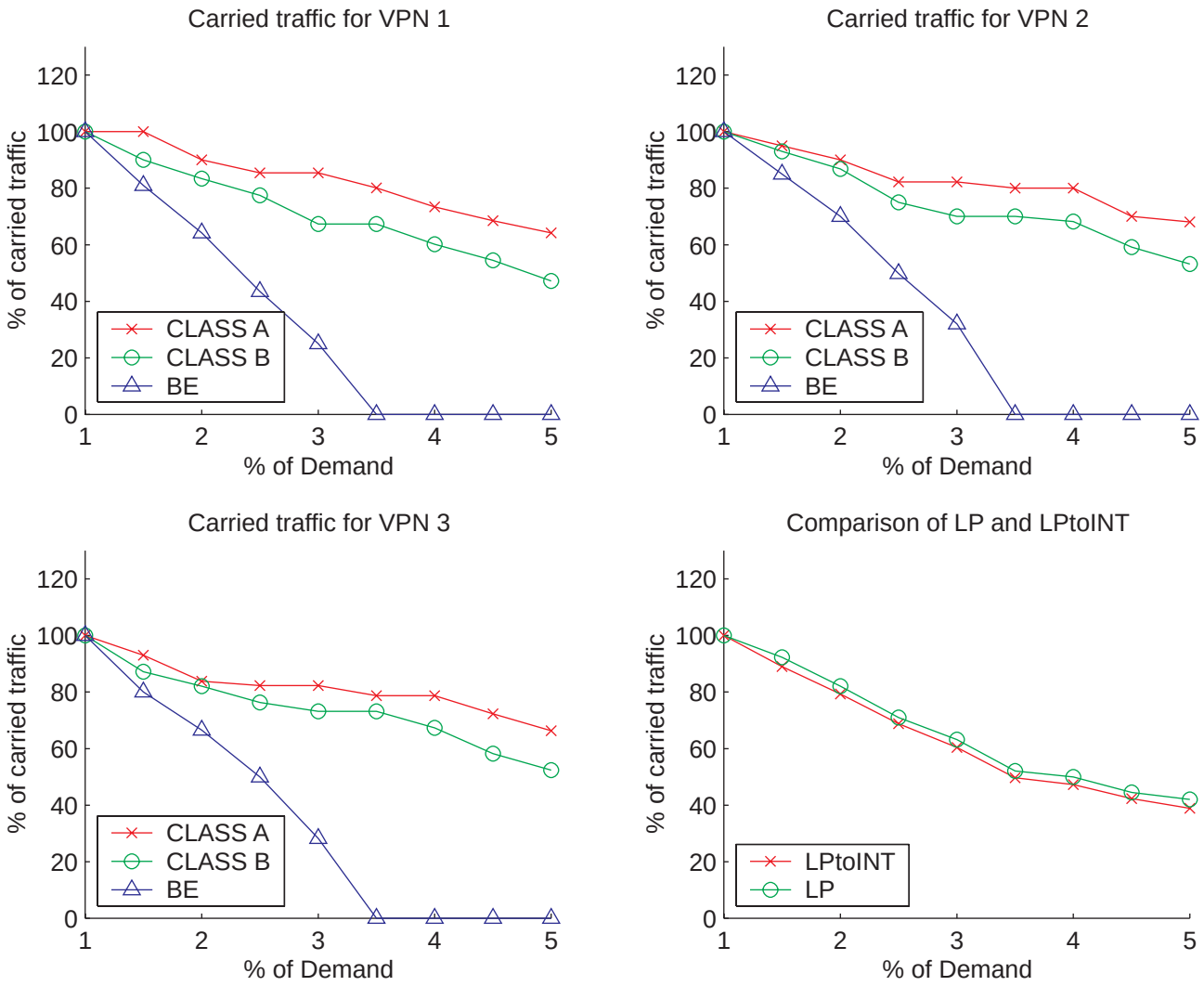

Figure 3.2: 1+1 link disjoint path protection with B_σ for Network 1

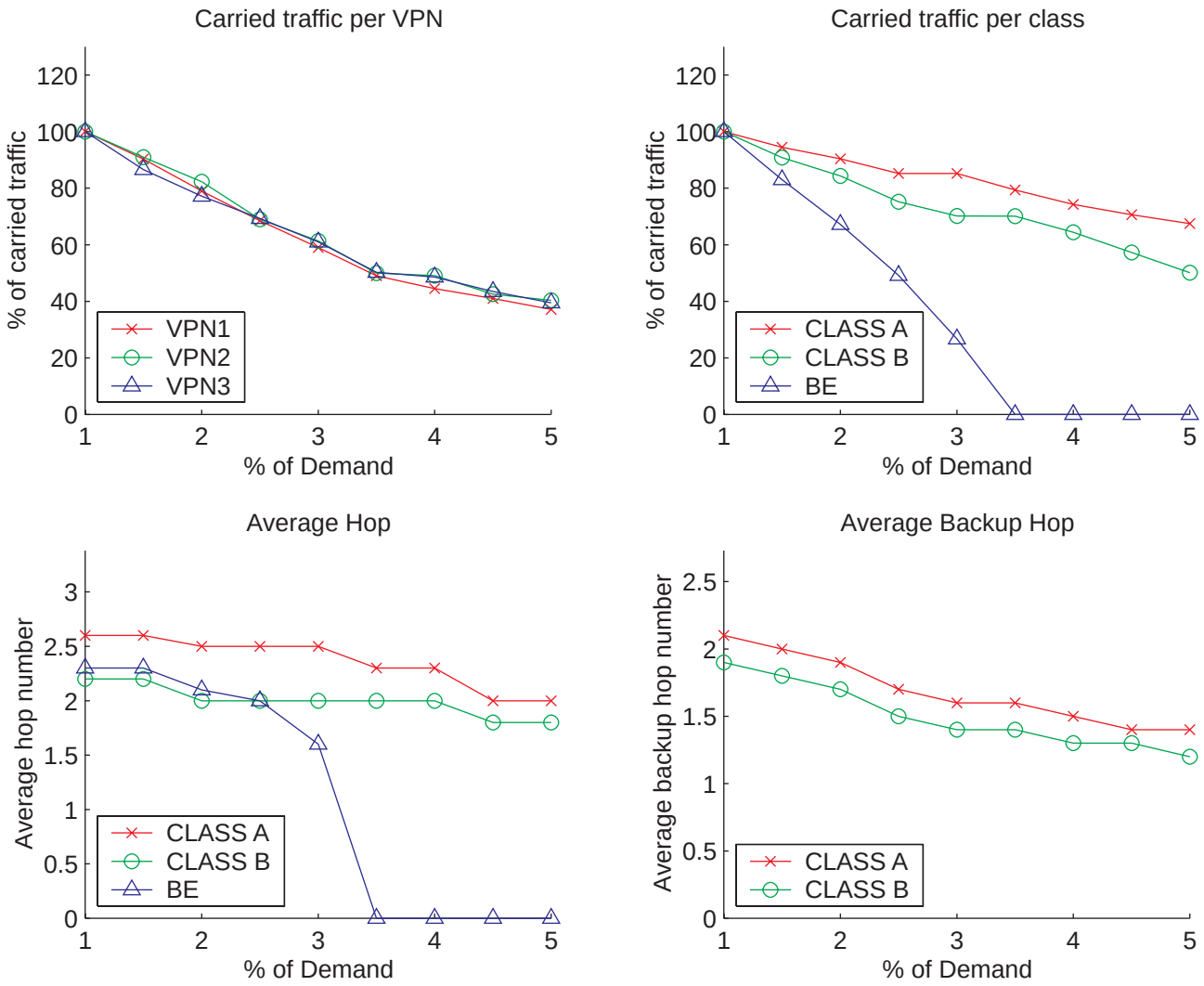

Figure 3.3: 1+1 link disjoint path protection without B_σ for Network 1

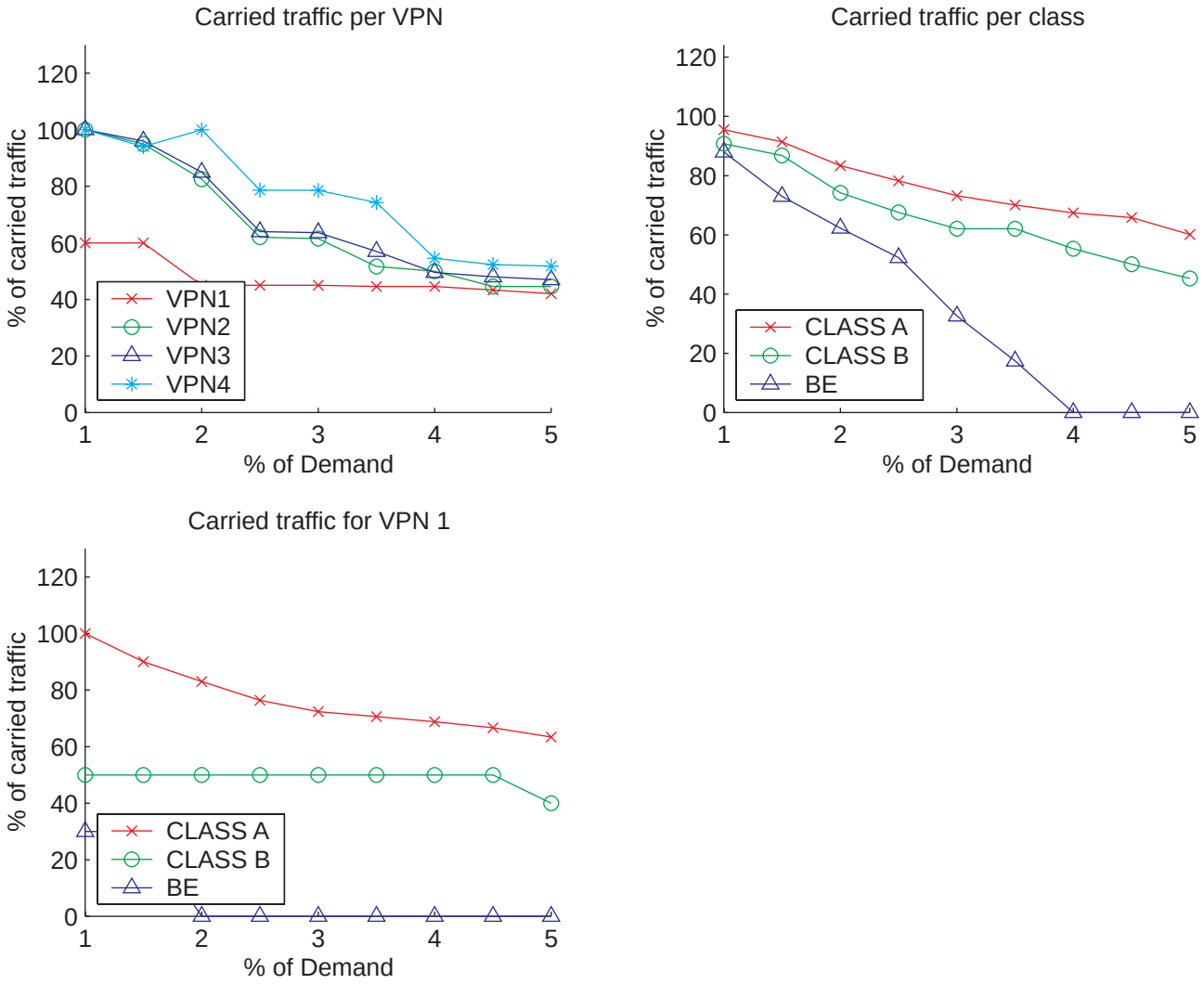

Figure 3.4: 1+1 link disjoint path protection with B_σ for Network 2

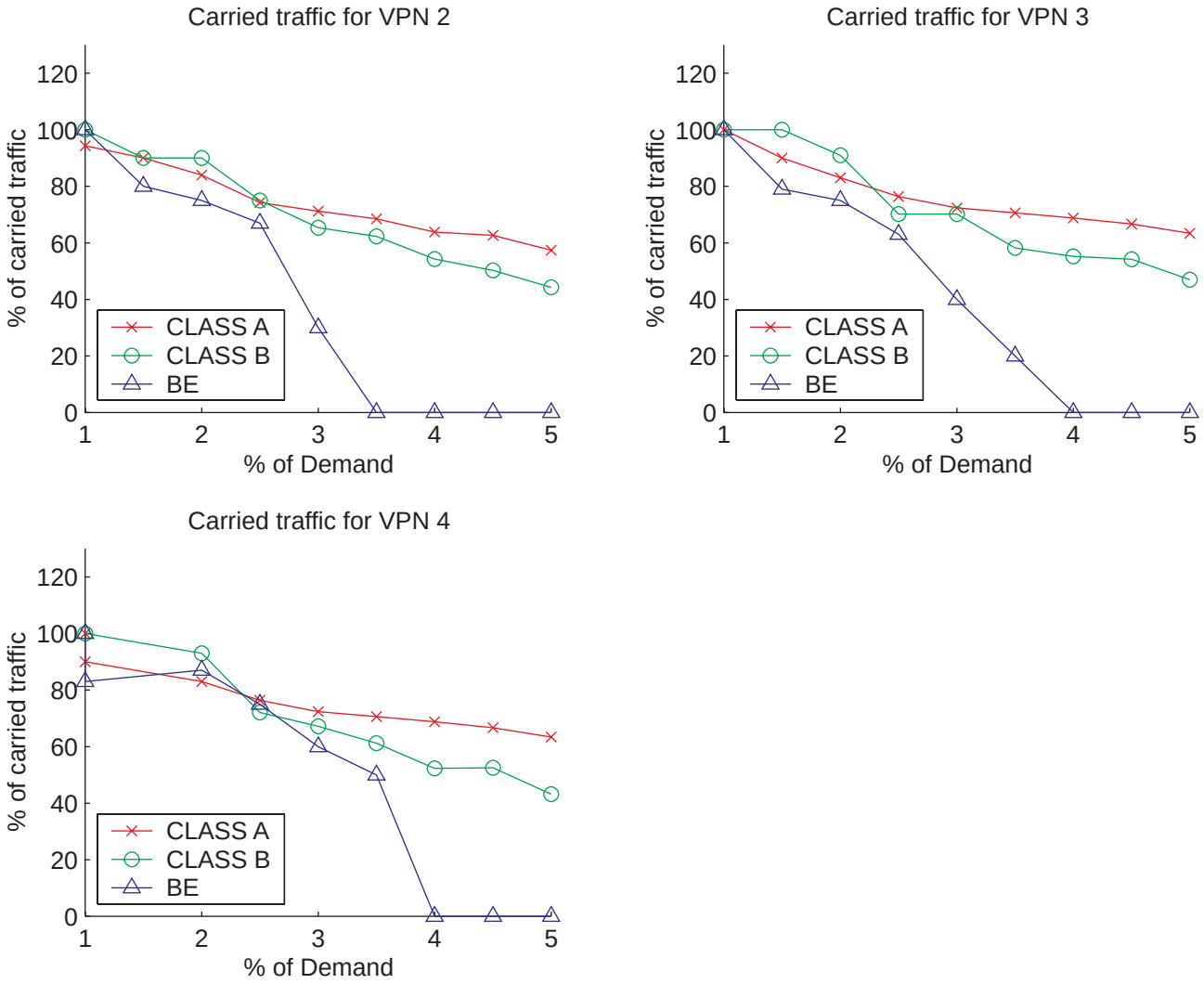

Figure 3.5: 1+1 link disjoint path protection with B_σ for Network 2

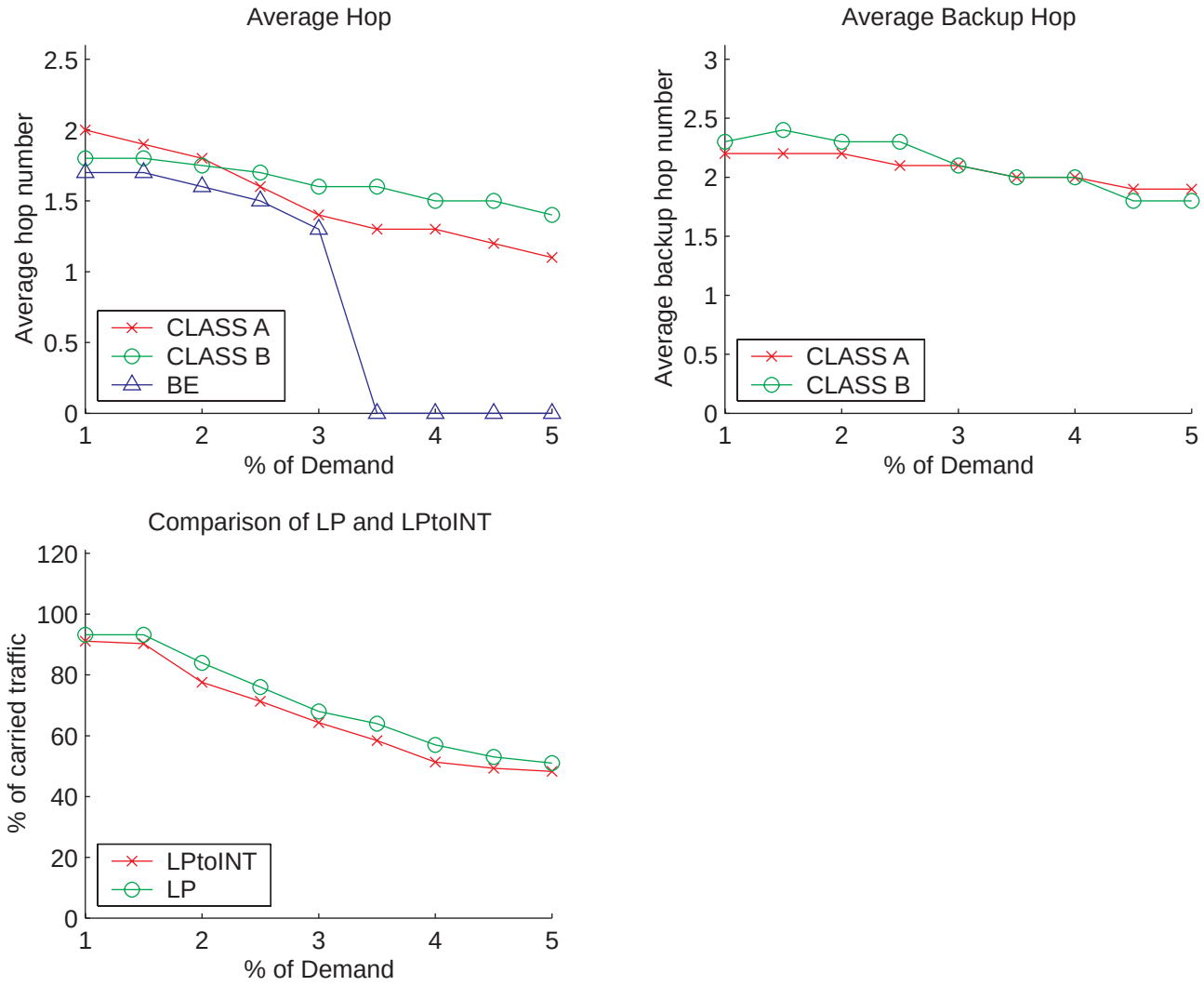

Figure 3.6: 1+1 link disjoint path protection with B_σ for Network 2

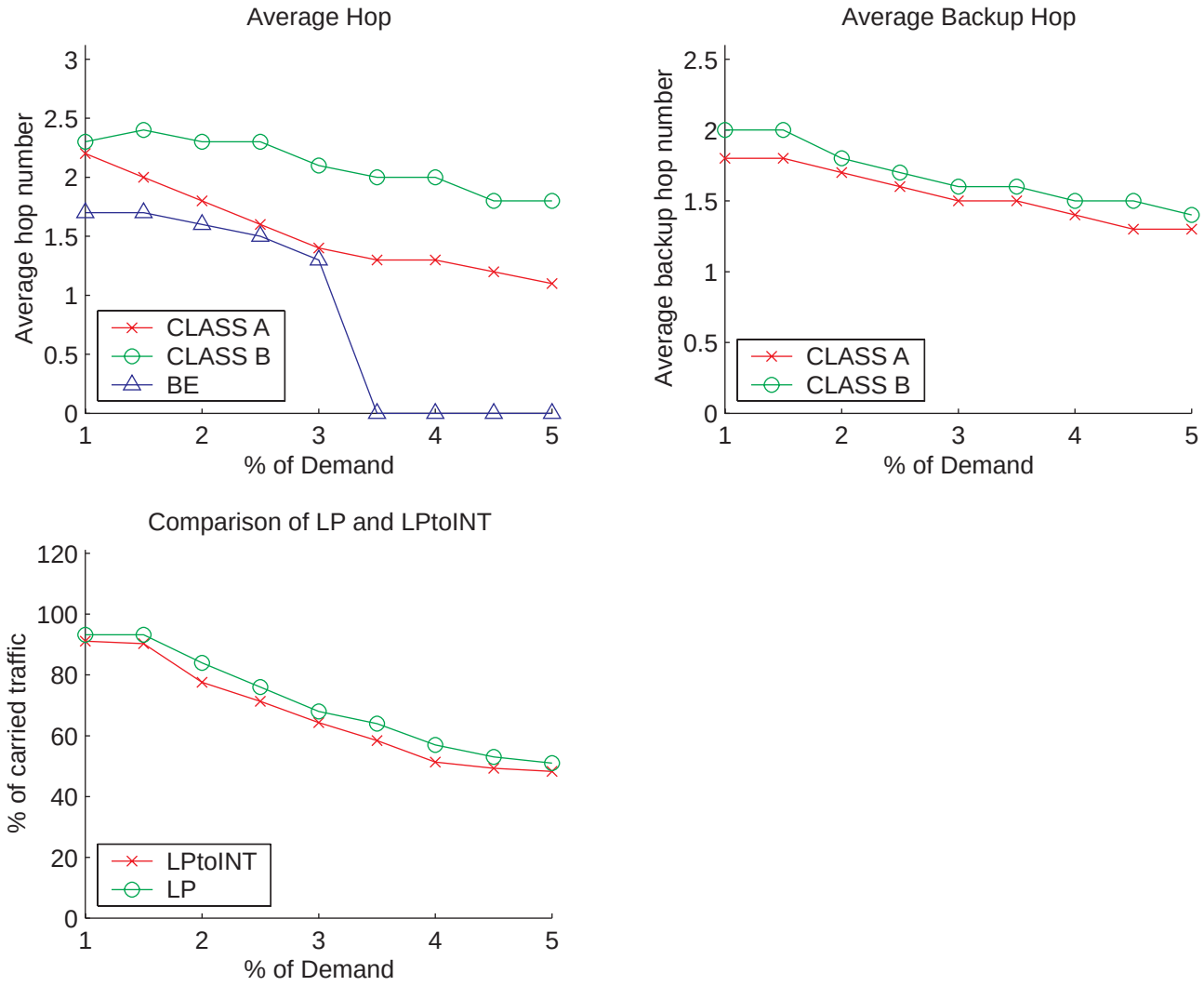

Figure 3.7: 1+1 link disjoint path protection without B_σ for Network 2

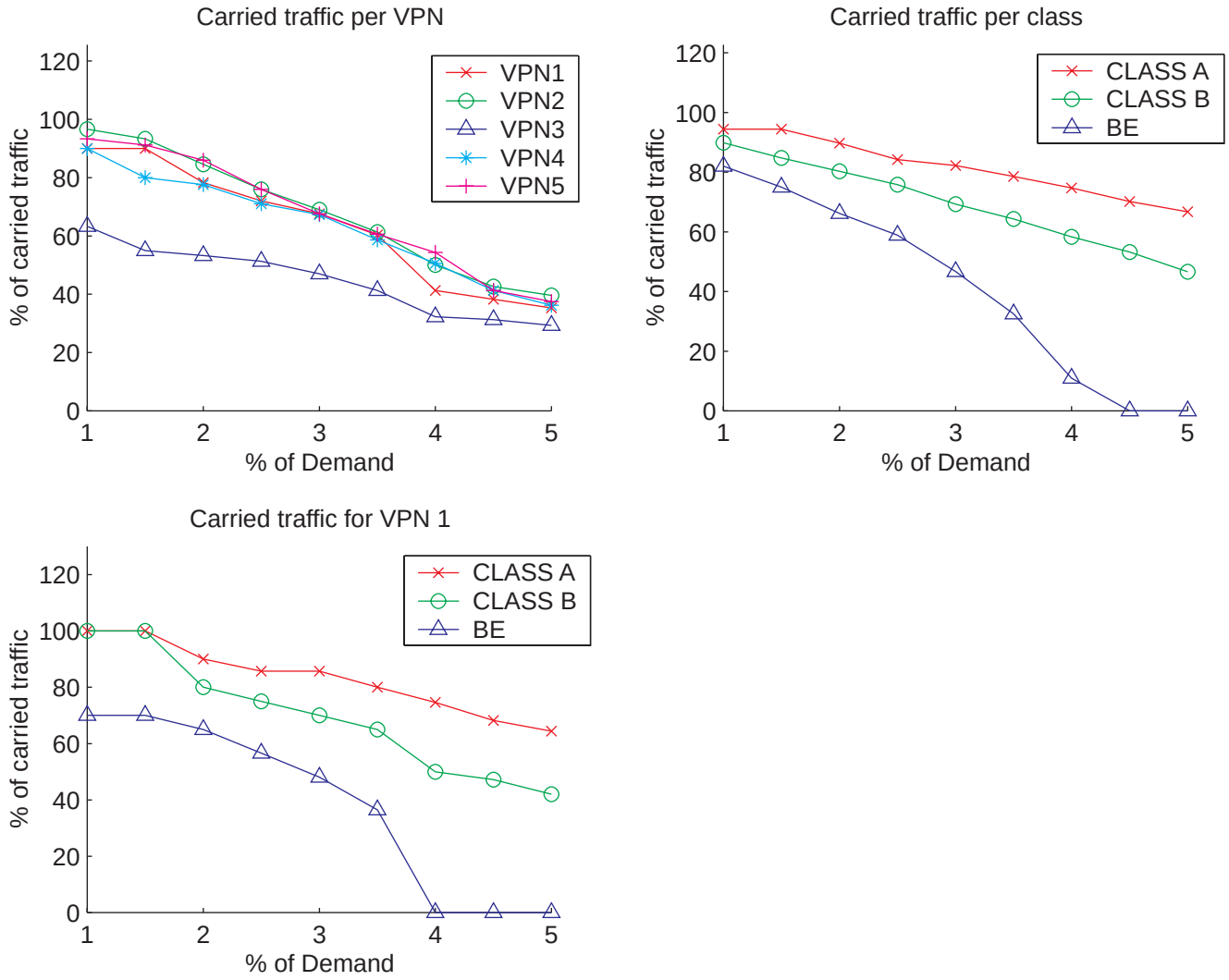

Figure 3.8: 1+1 link disjoint path protection with B_σ for Network 3

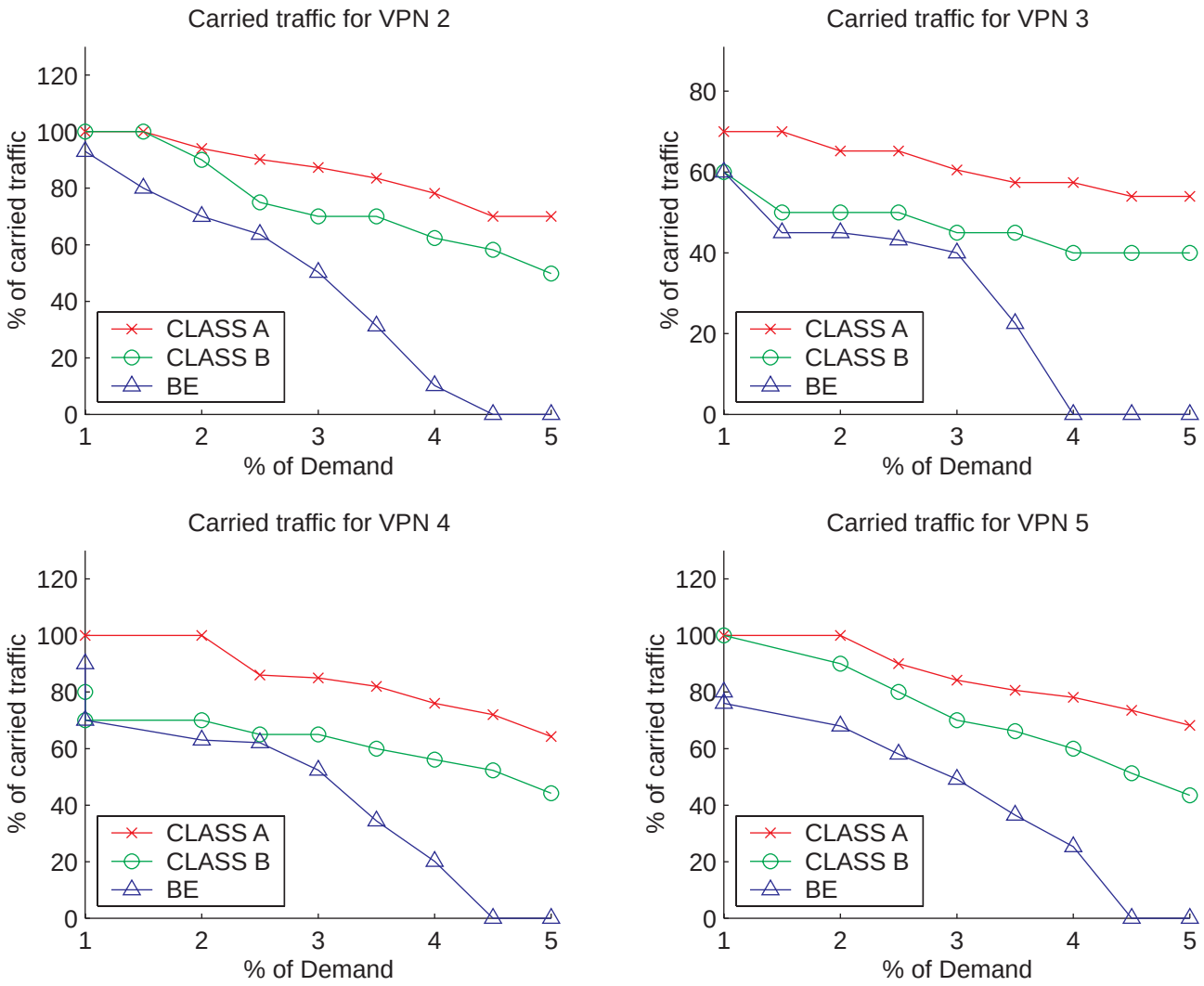

Figure 3.9: 1+1 link disjoint path protection with B_σ for Network 3

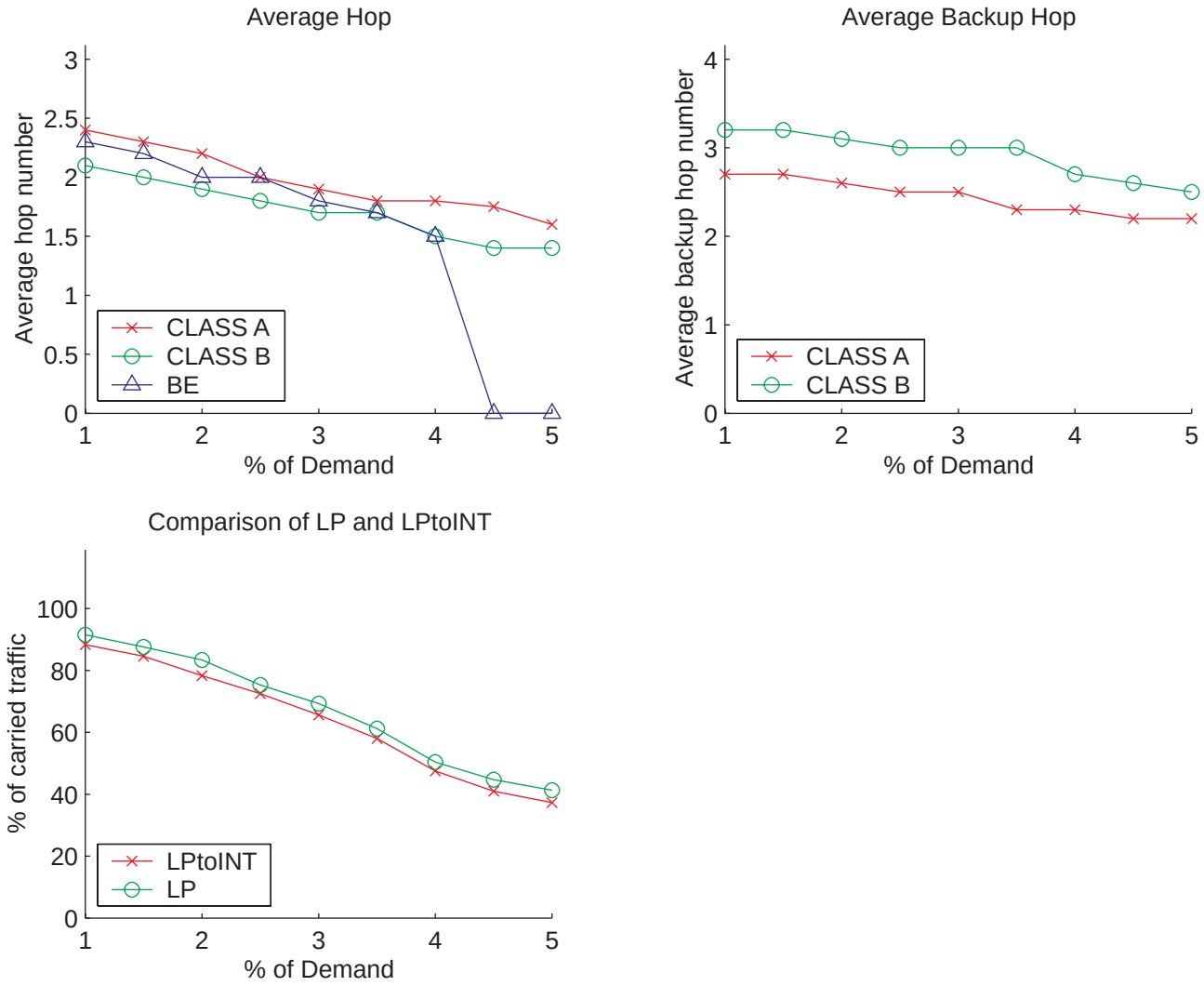

Figure 3.10: 1+1 link disjoint path protection with B_σ for Network 3

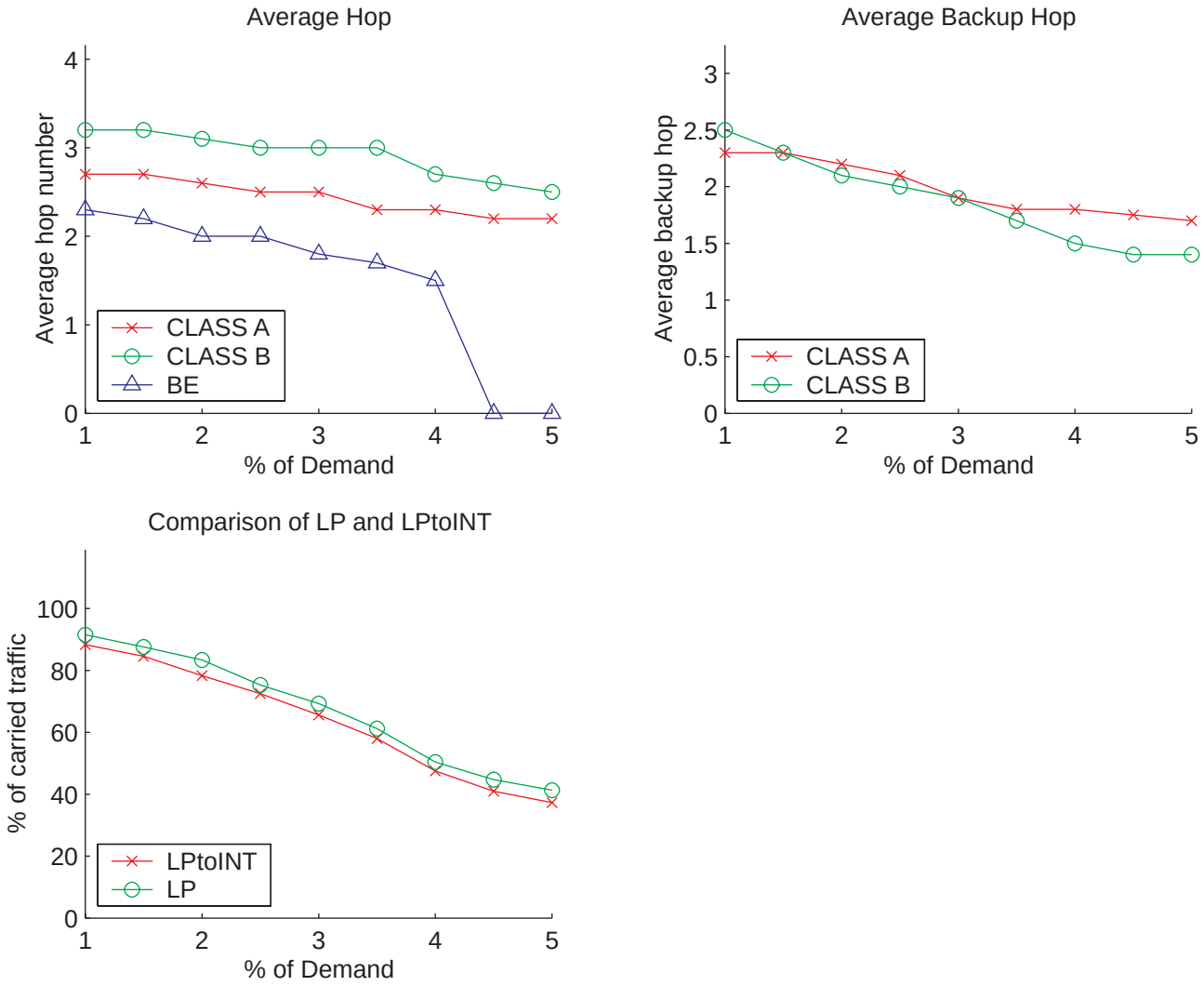

Figure 3.11: 1+1 link disjoint path protection without B_σ for Network 3

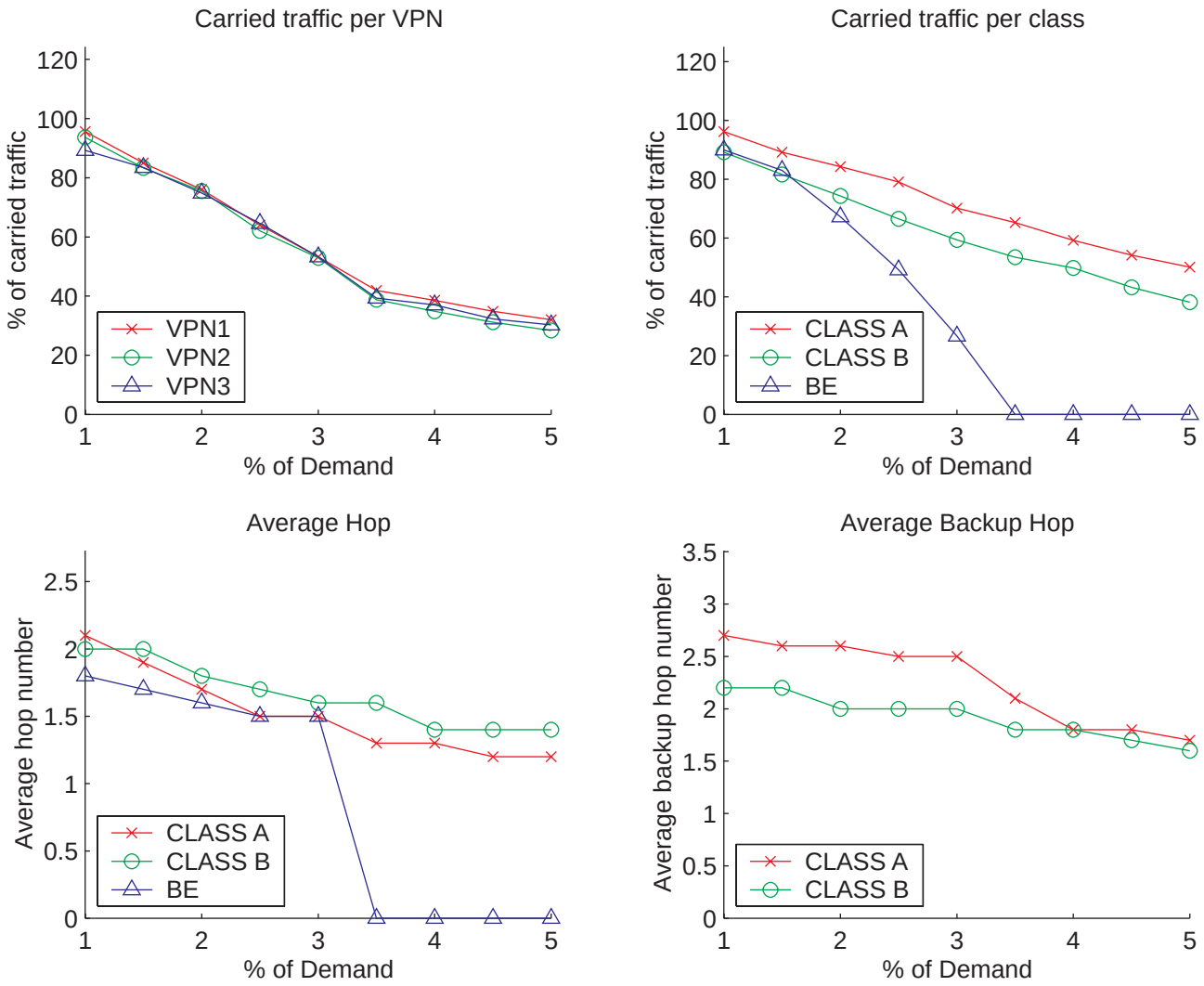

Figure 3.12: 1+1 node disjoint path protection with B_σ for Network 1

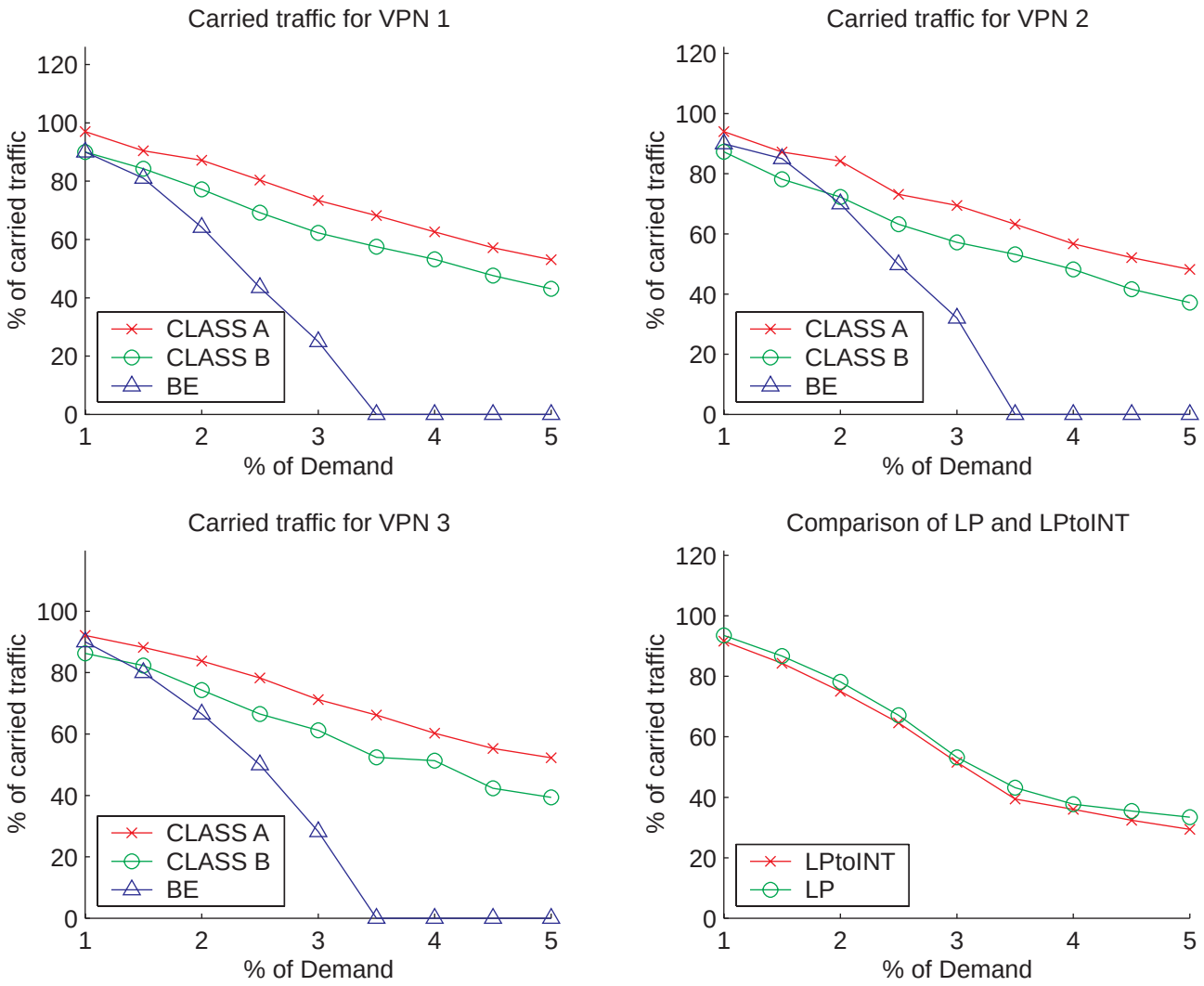

Figure 3.13: 1+1 node disjoint path protection with B_σ for Network 1

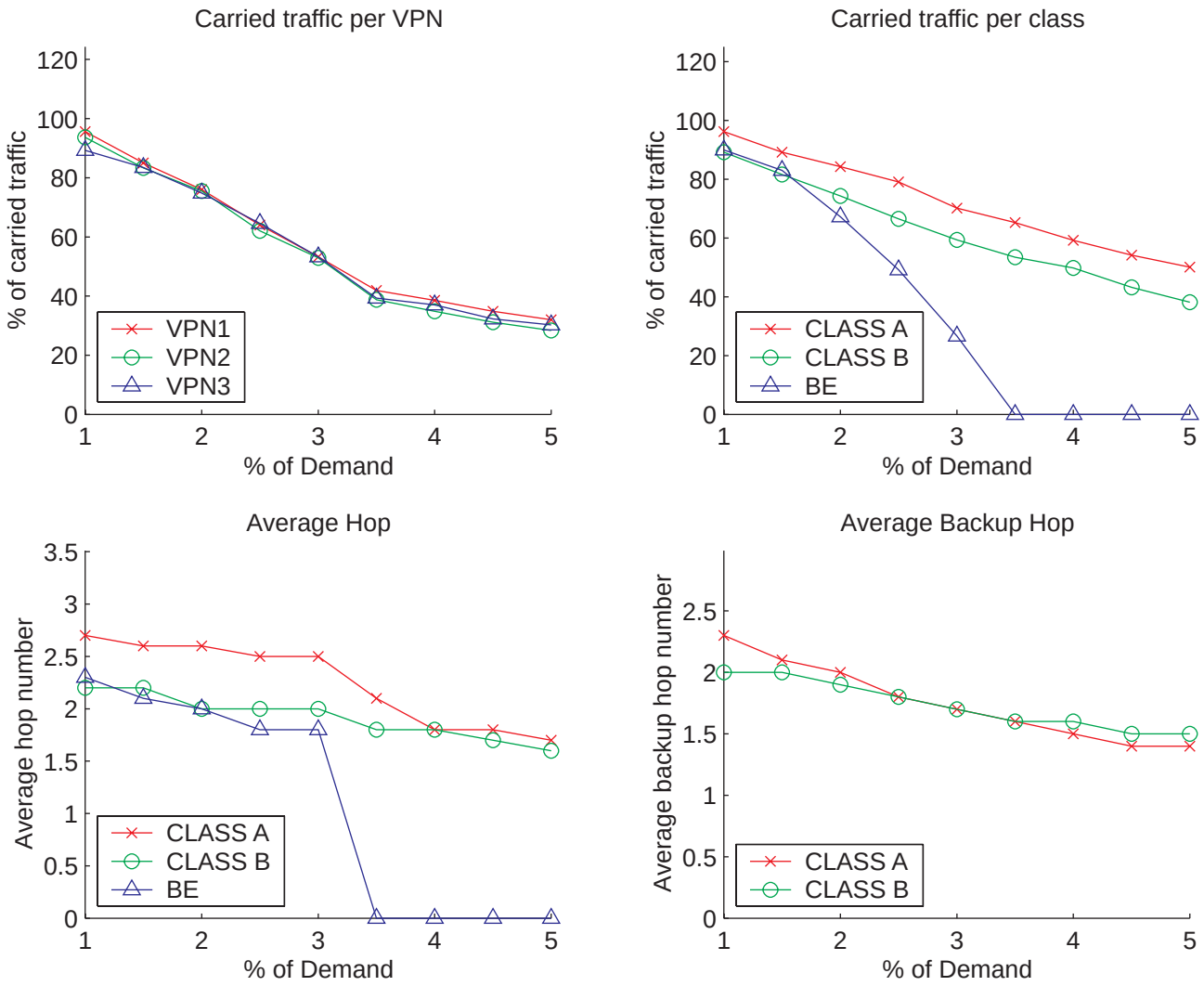

Figure 3.14: 1+1 node disjoint path protection without B_σ for Network 1

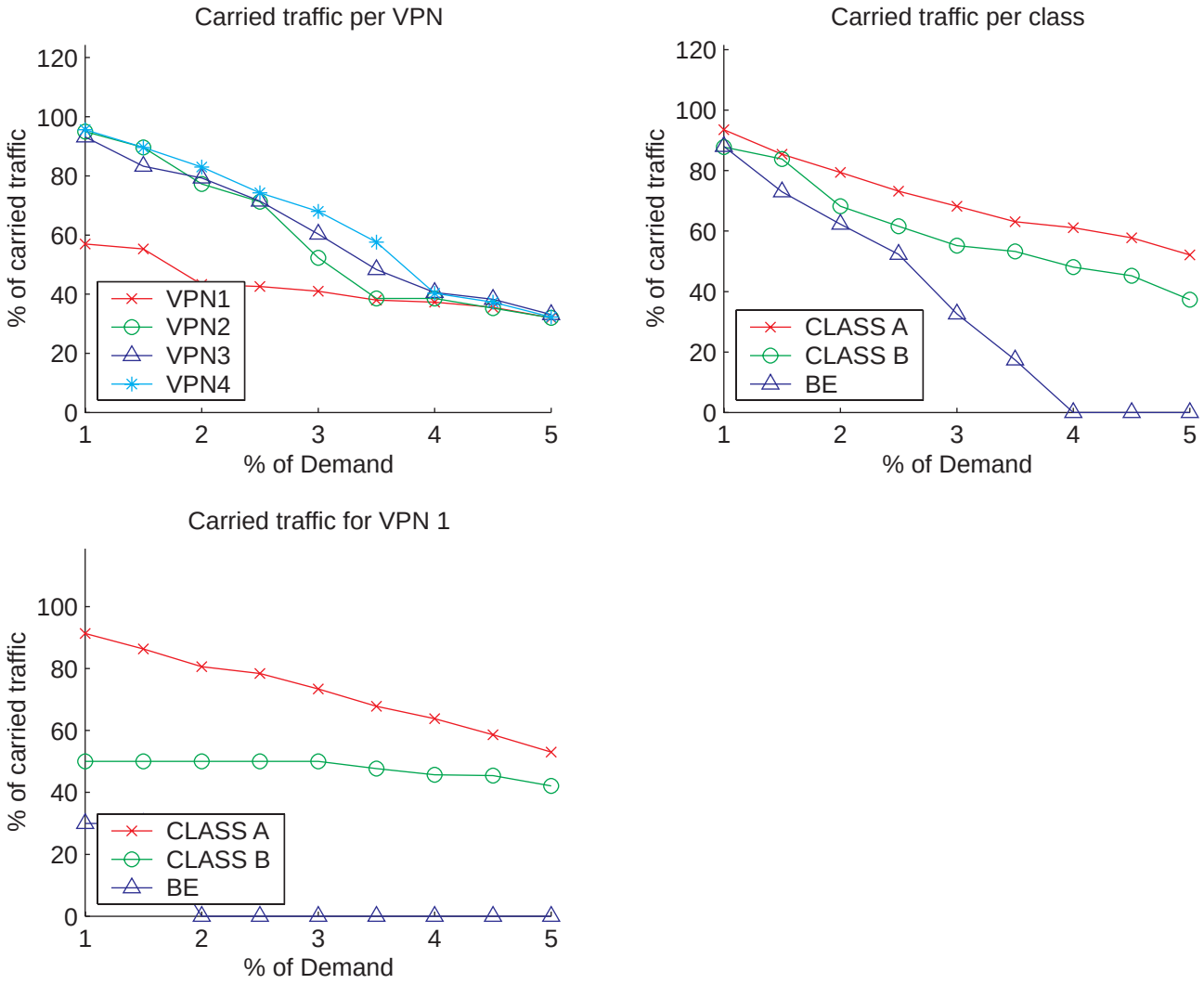

Figure 3.15: 1+1 node disjoint path protection with B_σ for Network 2

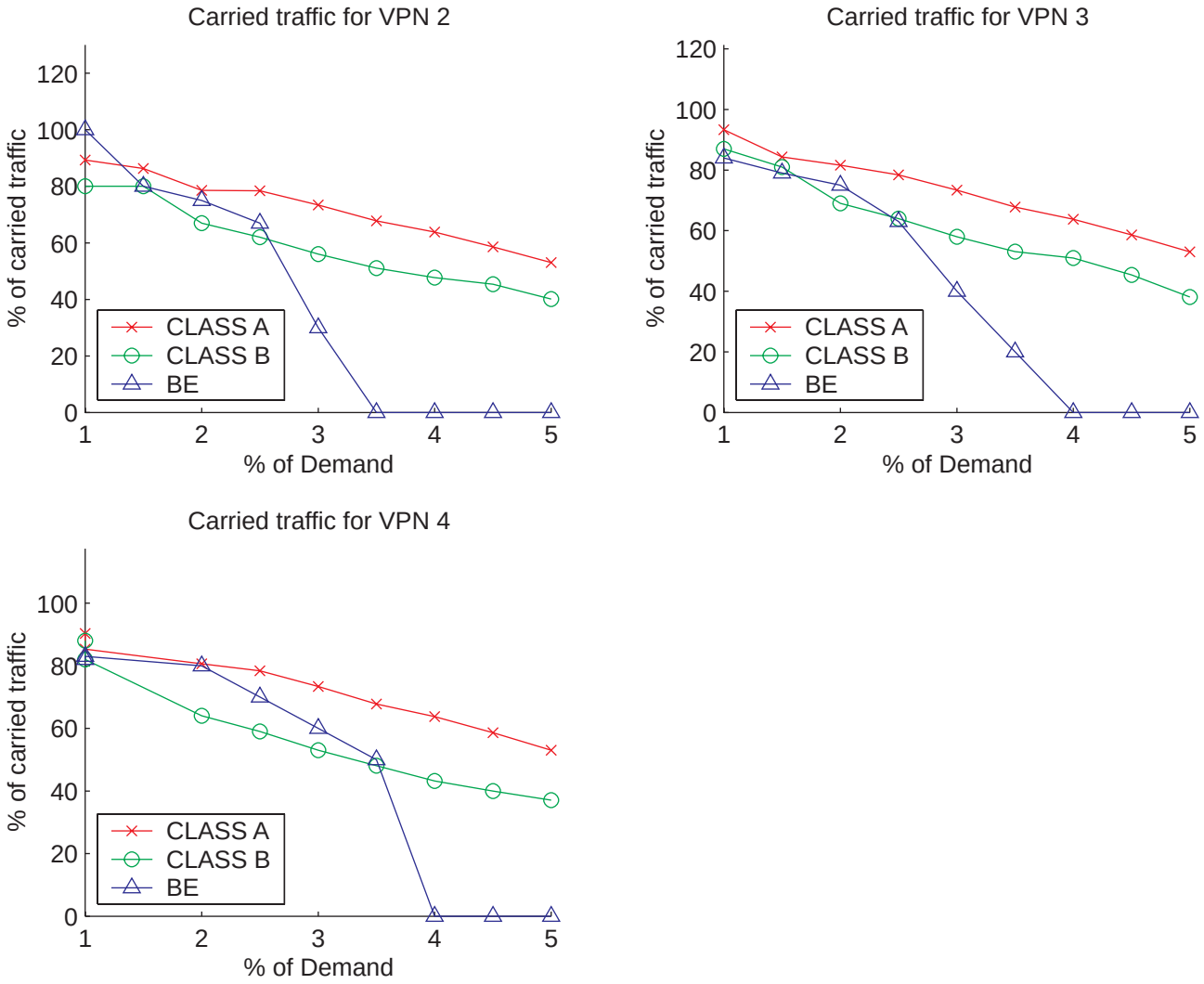

Figure 3.16: 1+1 node disjoint path protection with B_σ for Network 2

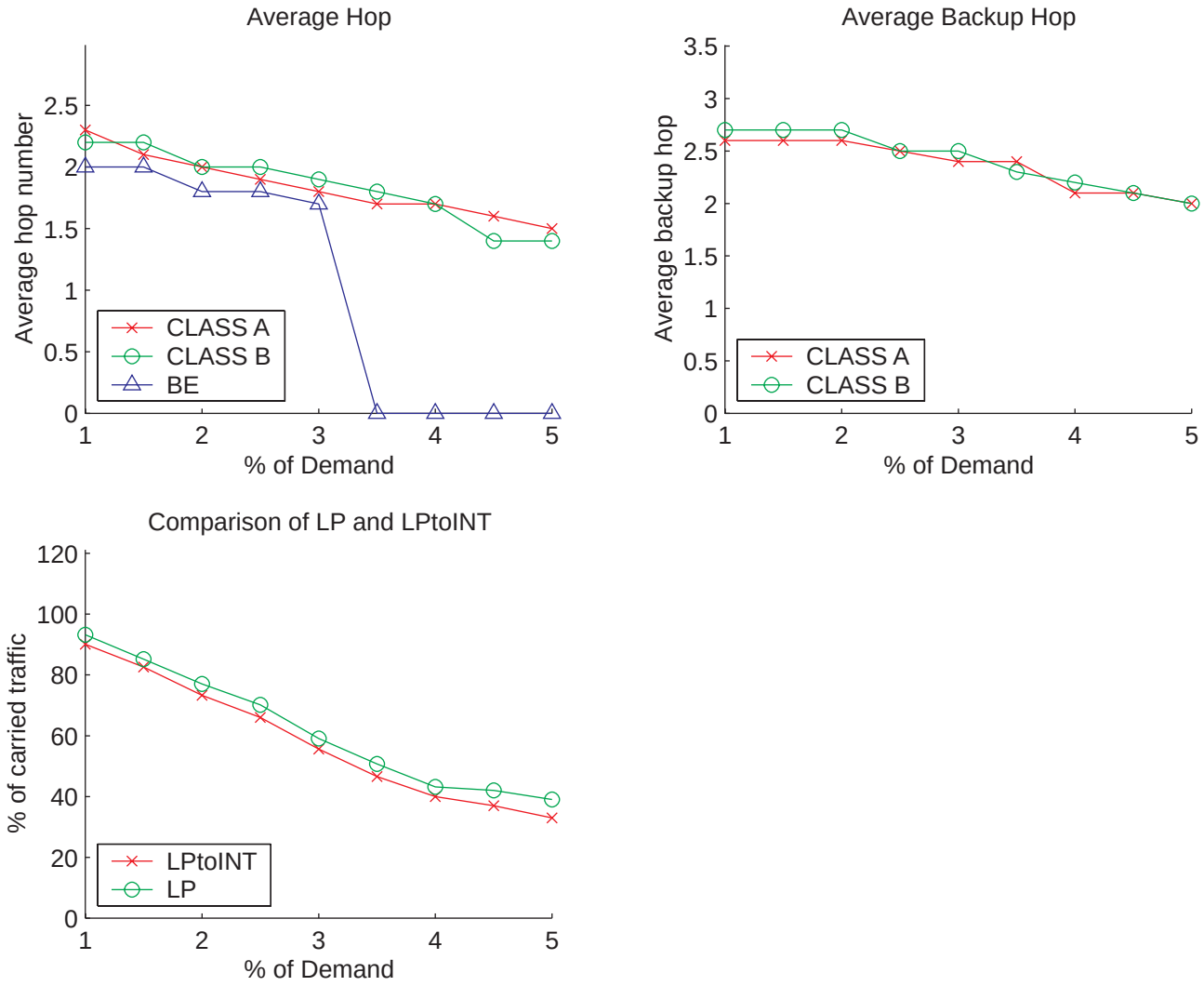

Figure 3.17: 1+1 node disjoint path protection with B_σ for Network 2

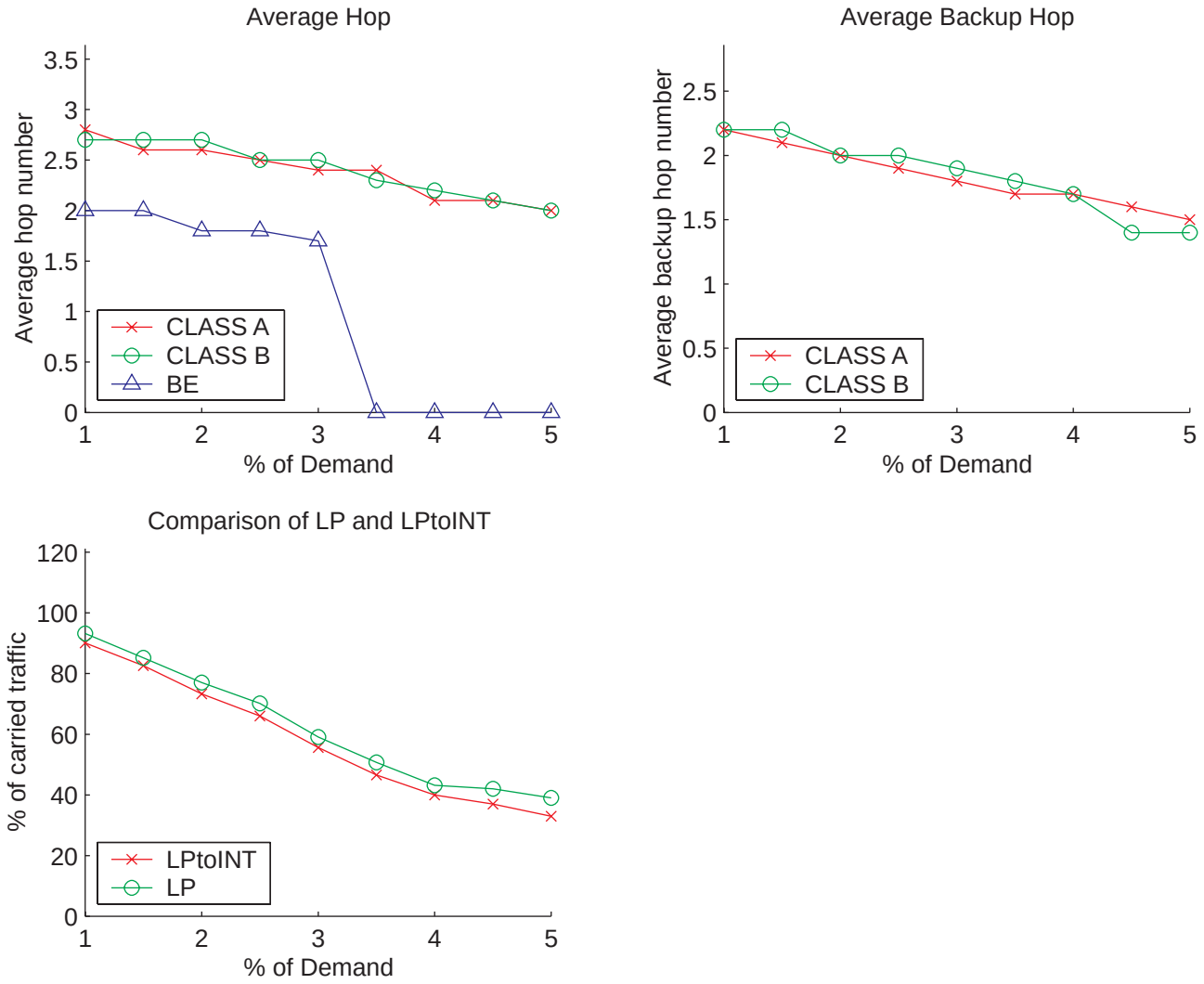

Figure 3.18: 1+1 node disjoint path protection without B_σ for Network 2

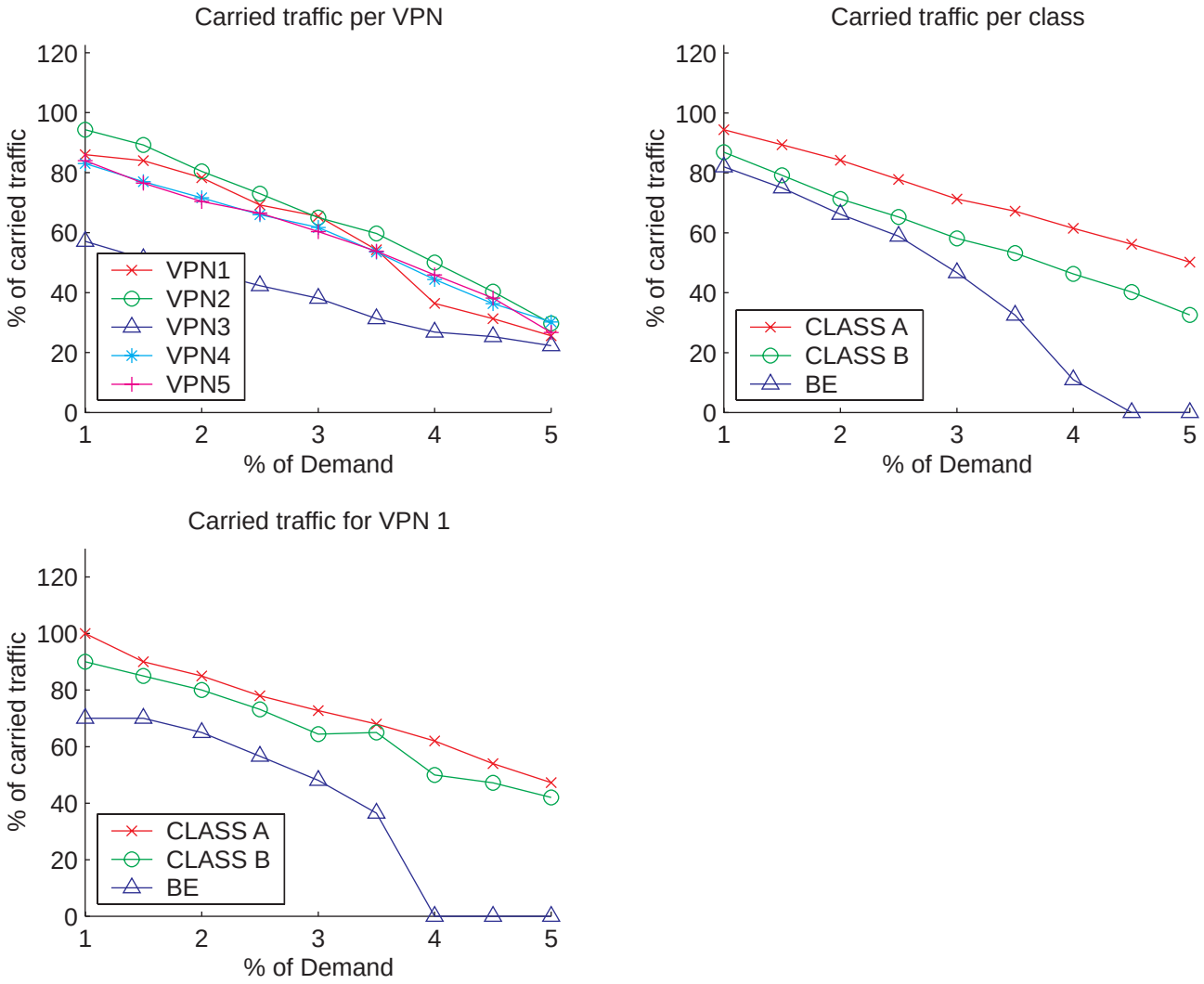

Figure 3.19: 1+1 node disjoint path protection with B_σ for Network 3

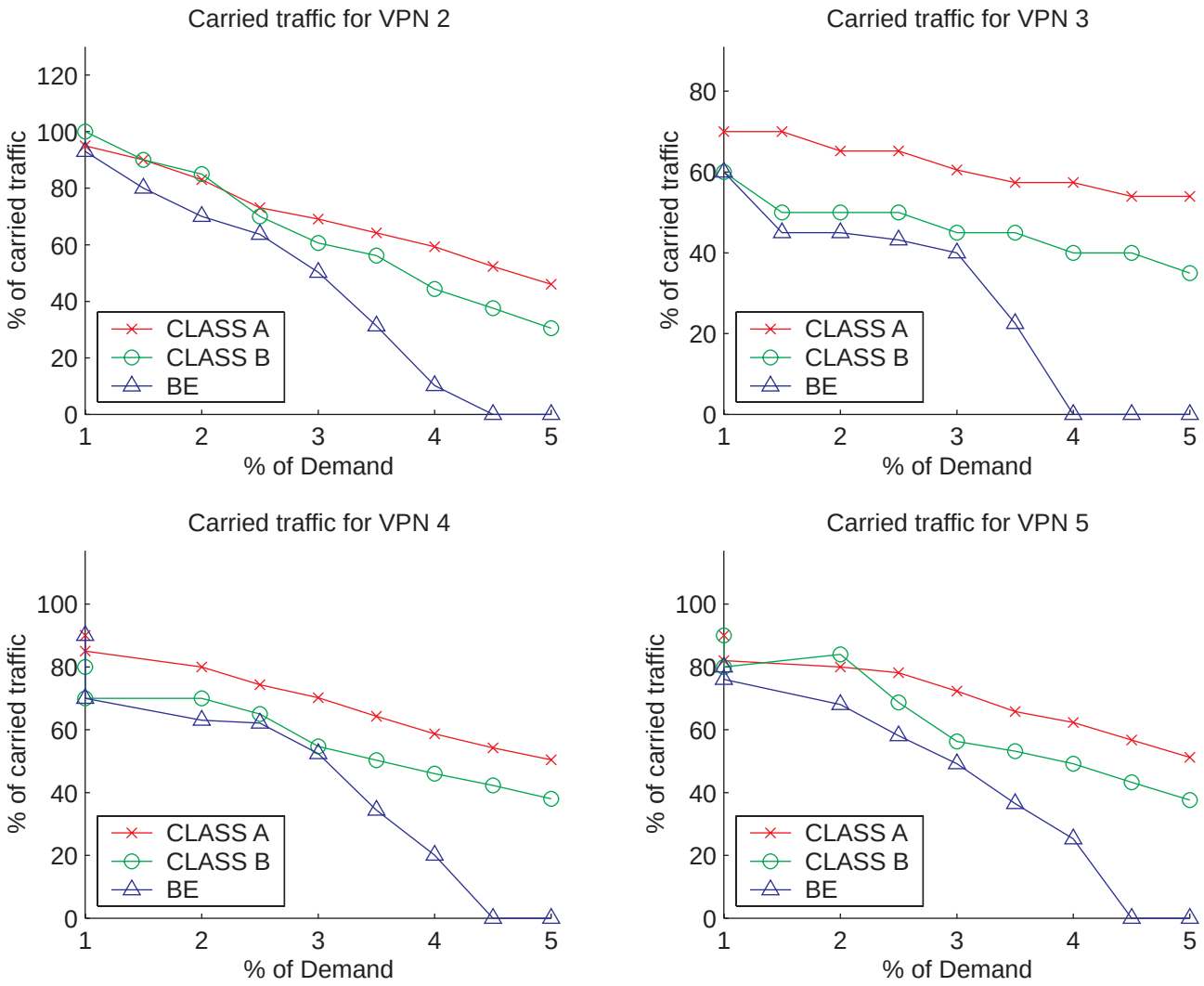

Figure 3.20: 1+1 node disjoint path protection with B_σ for Network 3

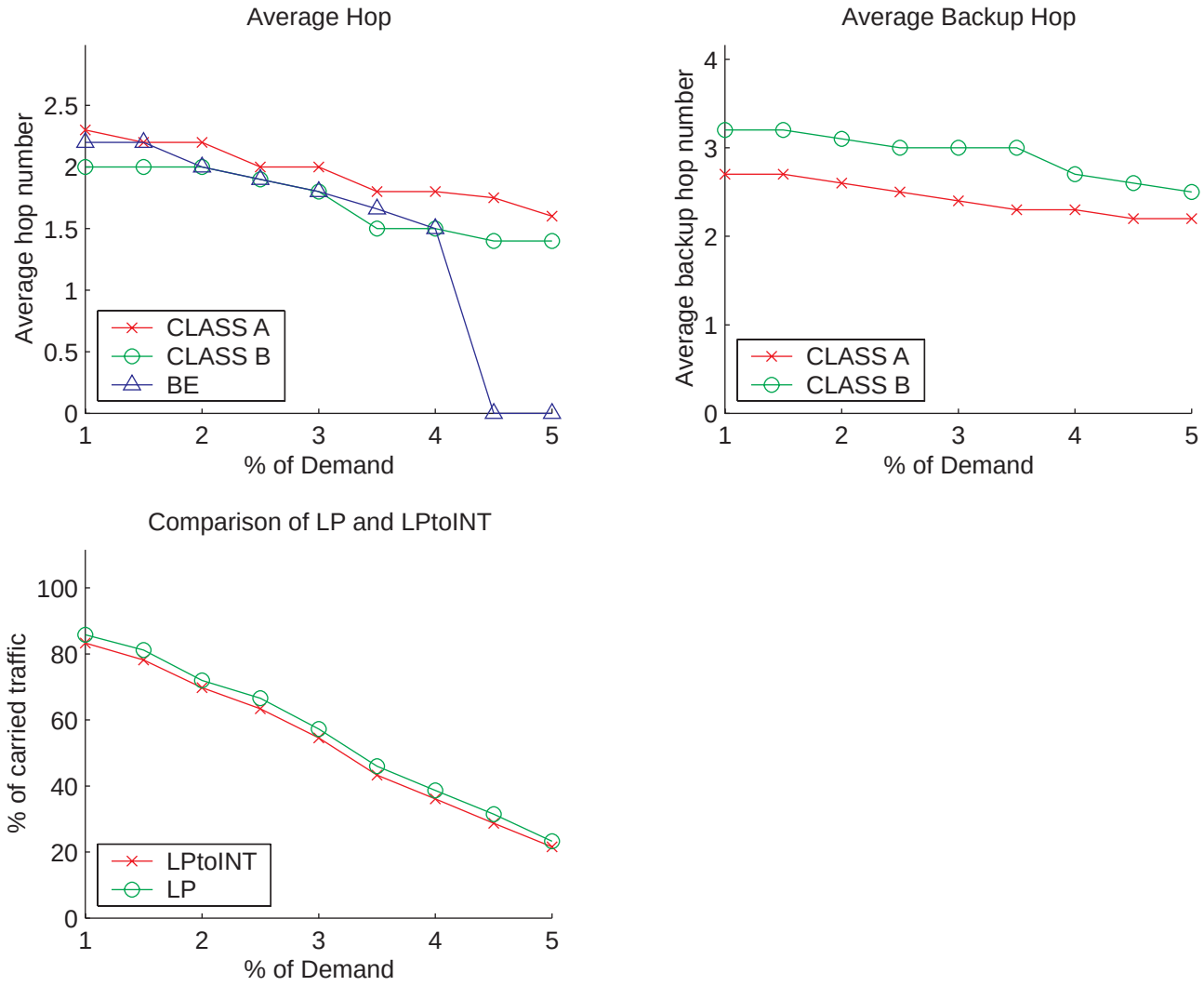

Figure 3.21: 1+1 node disjoint path protection with B_σ for Network 3

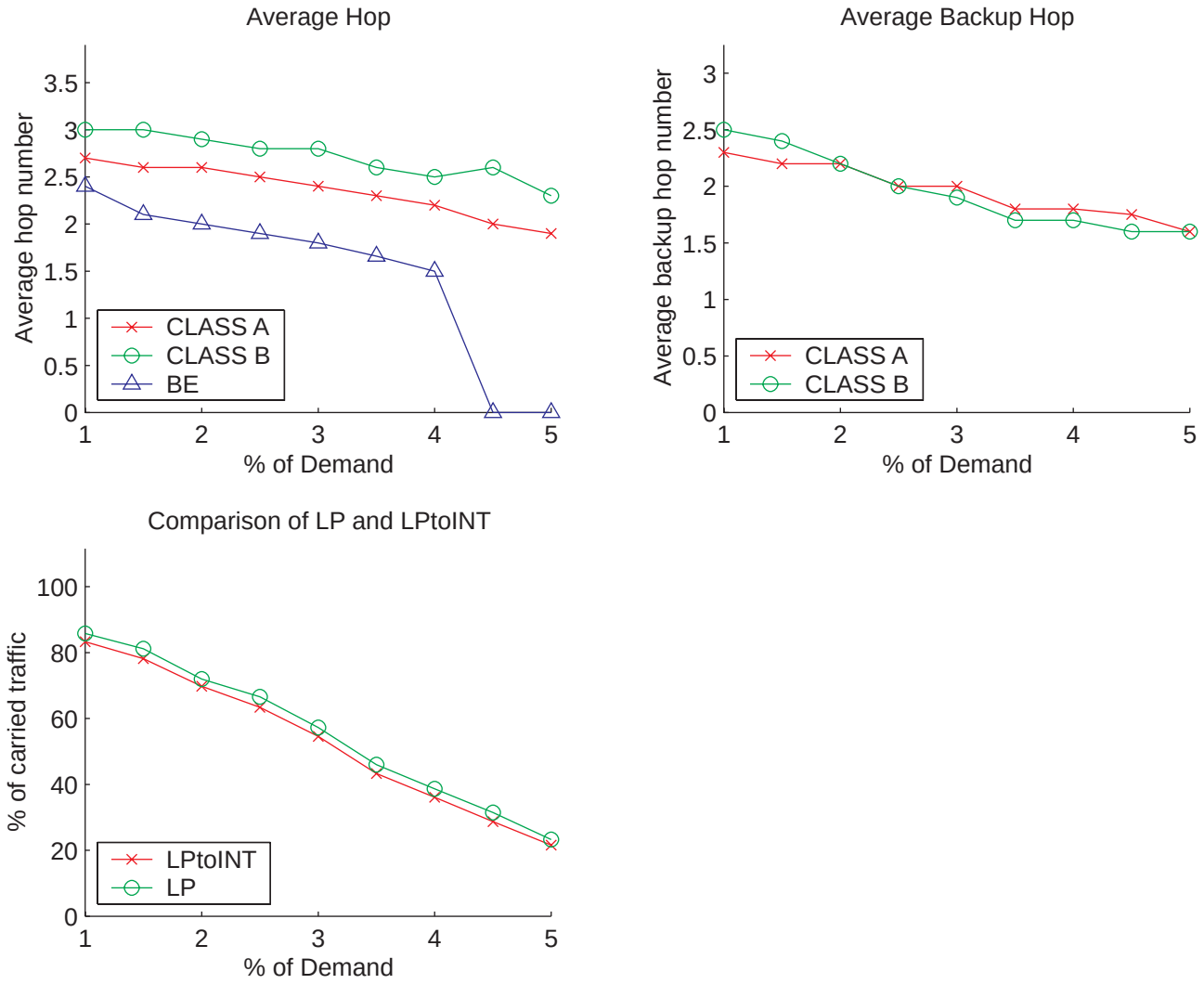

Figure 3.22: 1+1 node disjoint path protection without B_σ for Network 3

- $1:1$ **Link Disjoint Path Protection**

In Figures 3.23 - 3.24 we show the results of $1:1$ link-disjoint path protection scheme with B_σ for network 1. In Figures 3.26 - 3.28 we show the results of $1:1$ link-disjoint path protection scheme with B_σ for network 2. In Figures 3.30 - 3.32 we show the results of $1:1$ link-disjoint path protection scheme with B_σ for network 3.

The percentage of carried traffic, average hop number and backup average hop number are plotted vs the percentage of demand.The results are shown both for LP and LP-to-INT. T As the traffic demand increases, the percentage of traffic carried drops. The percentage of traffic carried for the QoS classes of traffic is the same as in the $1+1$ path protection scheme. But, the BE traffic has a higher percentage of carried traffic. This is because the resources of the backup path are available to the BE traffic. It is seen that the average backup hop number is larger compared to the average hop number of working path. This shows that a longer path is selected for the backup path.It is also seen that as the demand increases the average hop number also drops. This is done to conserve resources as a longer path would utilize more resources.

In Figures 3.25, 3.29 and 3.33 we show the $1:1$ link-disjoint path protection scheme without differentiation between the working path and backup path i.e without the parameter B_σ . We observe from the graphs that the average backup hop number is smaller compared the average hop number of working path showing the effect of B_σ.

- $1:1$ **Node Disjoint Path Protection**

In Figures 3.34 - 3.35 we show the results of $1:1$ node-disjoint path protection scheme with B_σ for network 1. In Figures 3.37 - 3.39 we show the results of $1:1$ node-disjoint path protection scheme with B_σ for network 2. In Figures 3.41 - 3.43 we show the results of $1:1$ node-disjoint path protection scheme with B_σ for network 3.

The percentage of carried traffic, average hop number and backup average hop number vs the percentage of the demand is plotted. The results are shown both for LP and LP-to-INT. The results are similar to link disjoint backup scheme except that the QoS traffic of each VPN is dropped earlier. This is because it is difficult to establish a node disjoint backup path. We see that the average hop number also drops as the demand increases as in the link protection scheme. The effect of the parameter B_σ is also seen.

In Figures 3.36, 3.40 and 3.44 we show the $1:1$ node-disjoint path protection scheme without differentiation between the working path and backup path i.e without the parameter B_σ . We observe from the graphs that the average backup hop number is smaller compared the average hop number of working path showing the effect of B_σ.

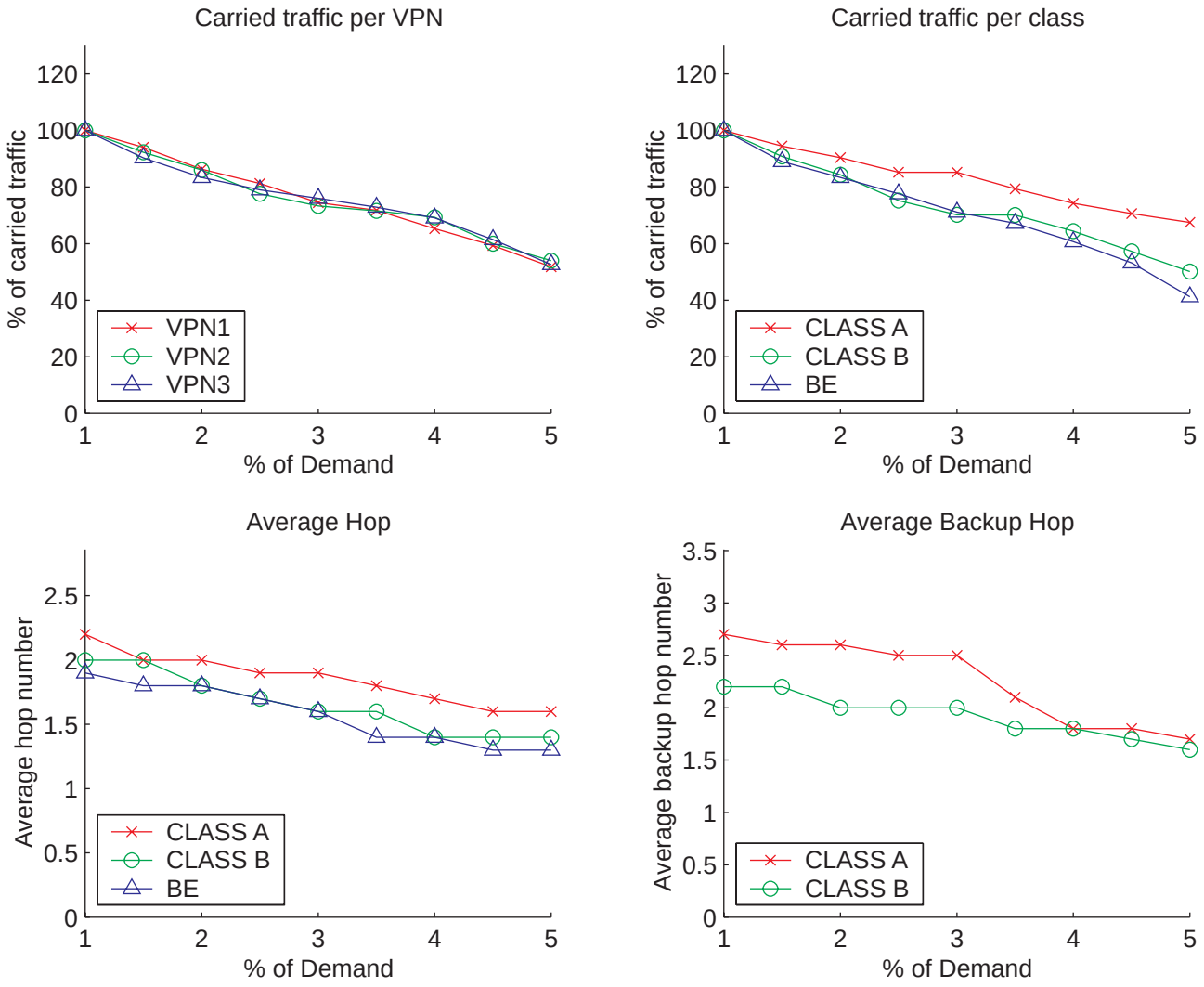

Figure 3.23: 1:1 link disjoint path protection with B_σ for Network 1

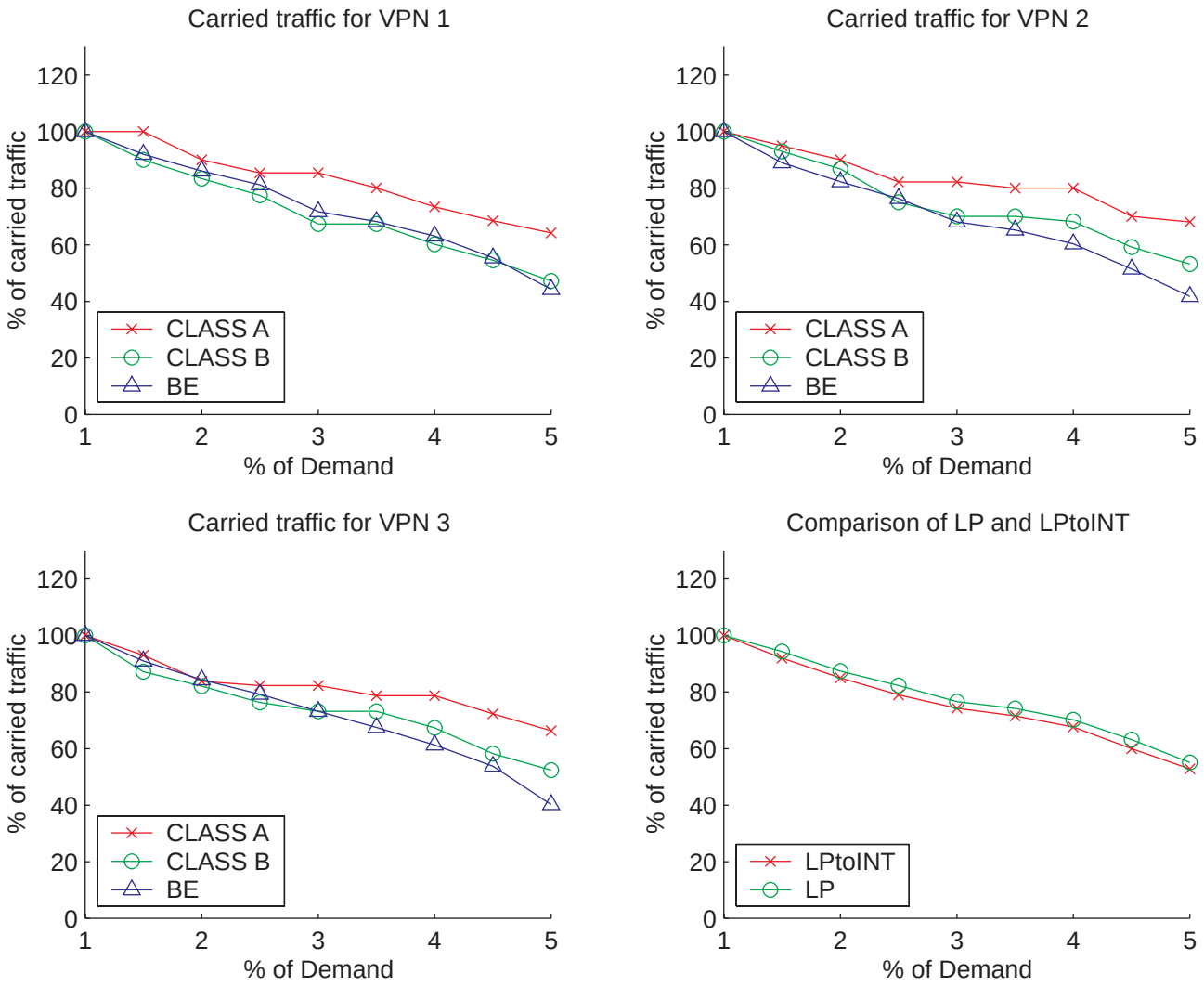

Figure 3.24: 1:1 link disjoint path protection with B_σ for Network 1

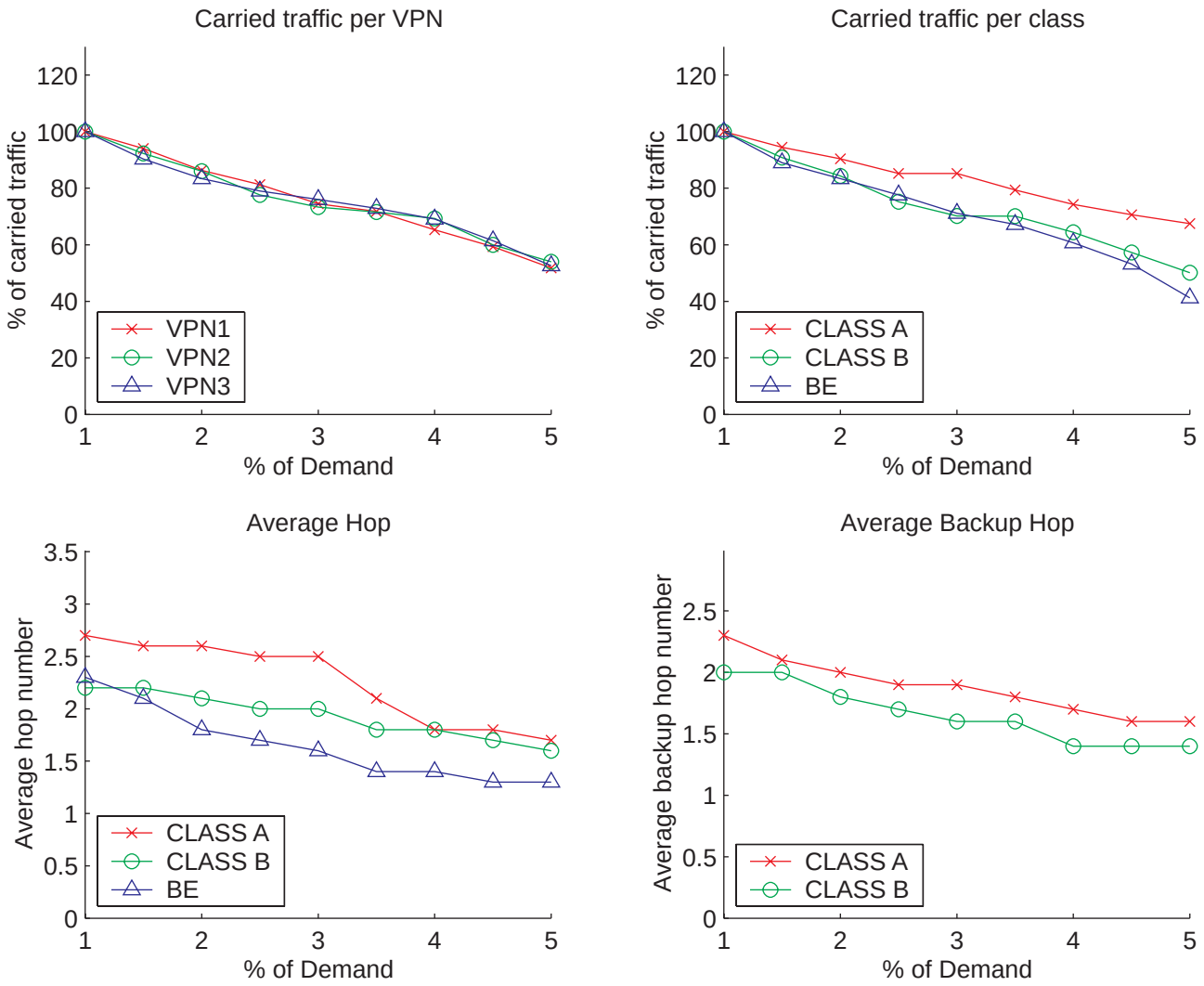

Figure 3.25: 1:1 link disjoint path protection without B_σ for Network 1

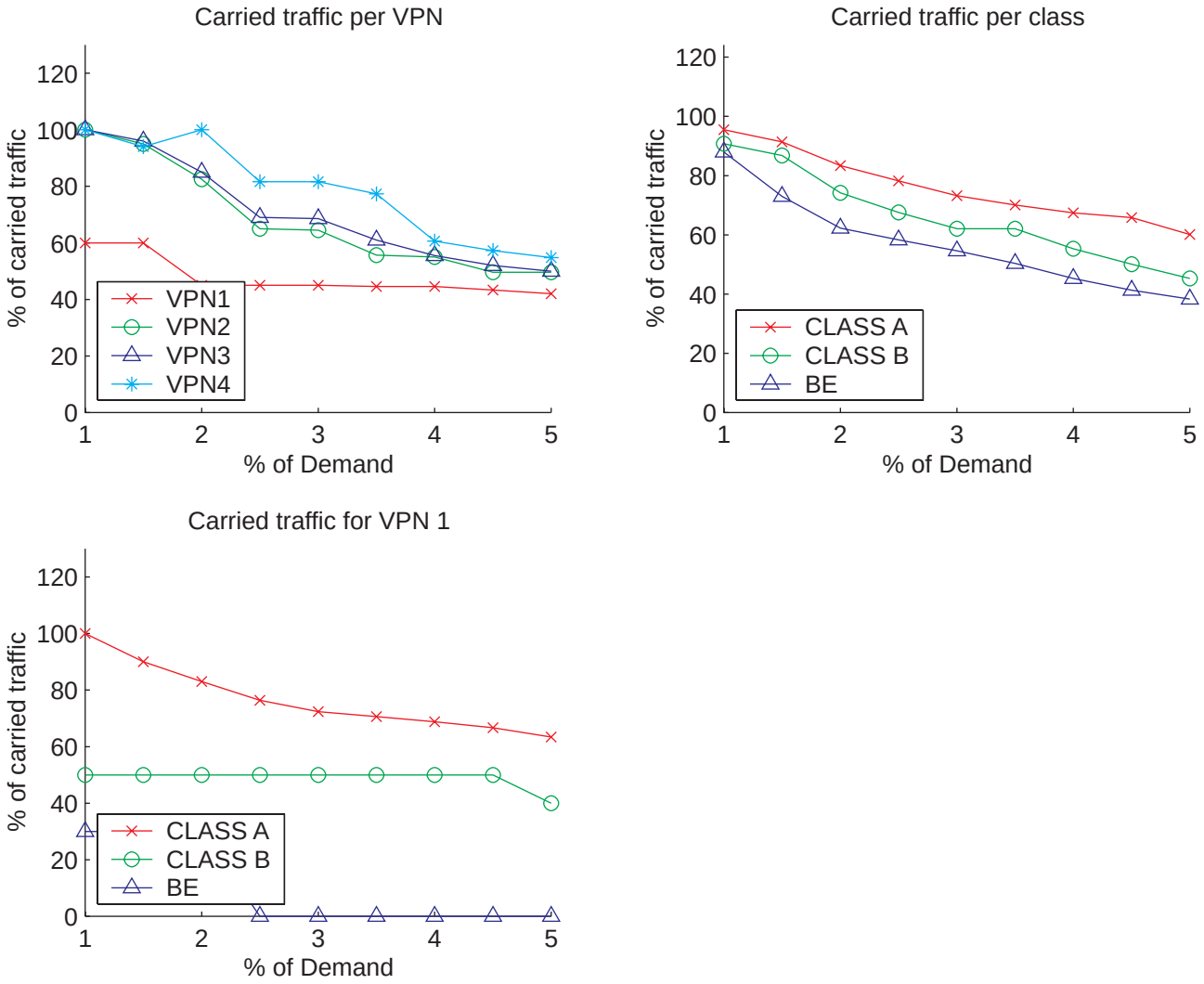

Figure 3.26: 1:1 link disjoint path protection with B_σ for Network 2

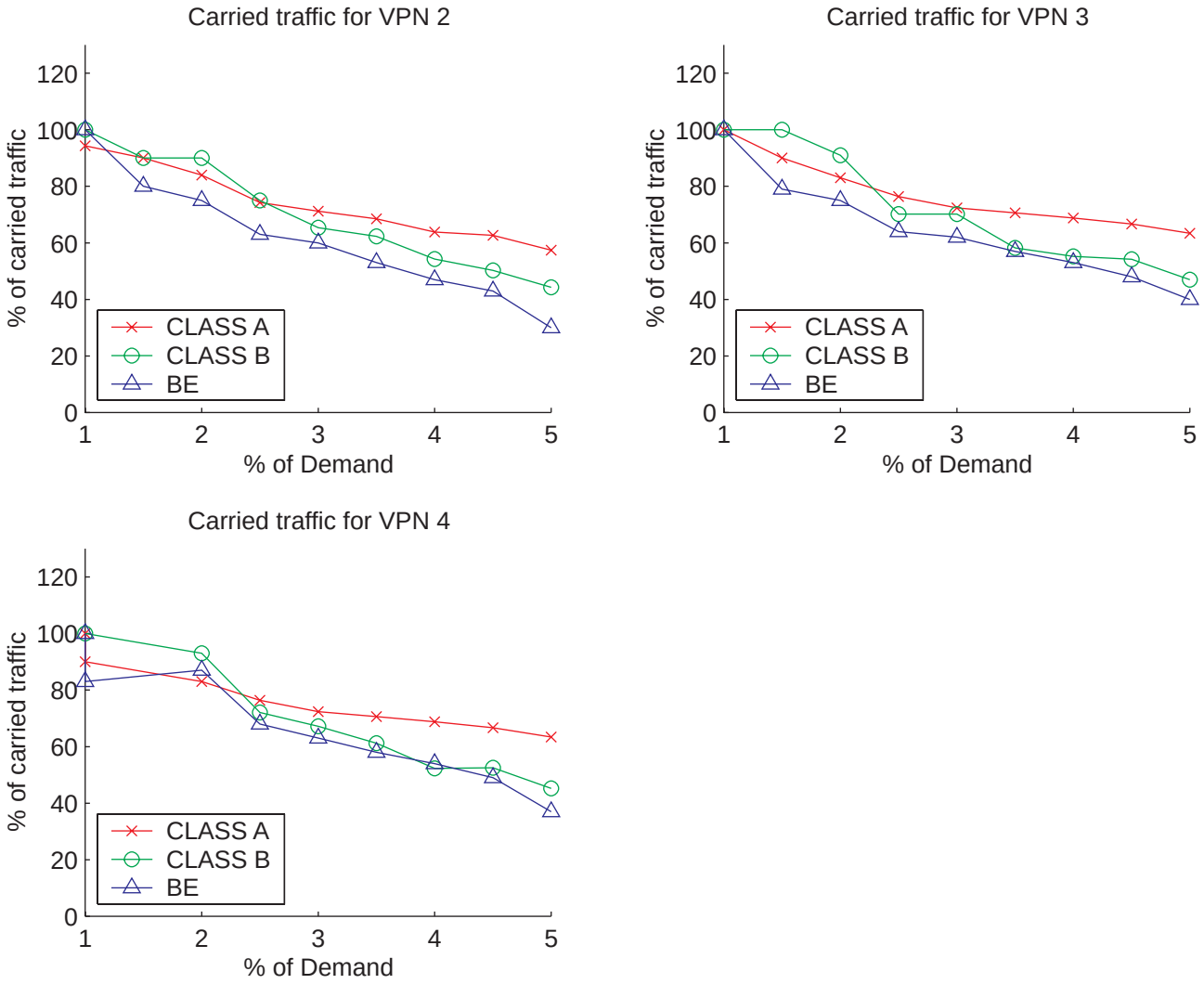

Figure 3.27: 1:1 link disjoint path protection with B_σ for Network 2

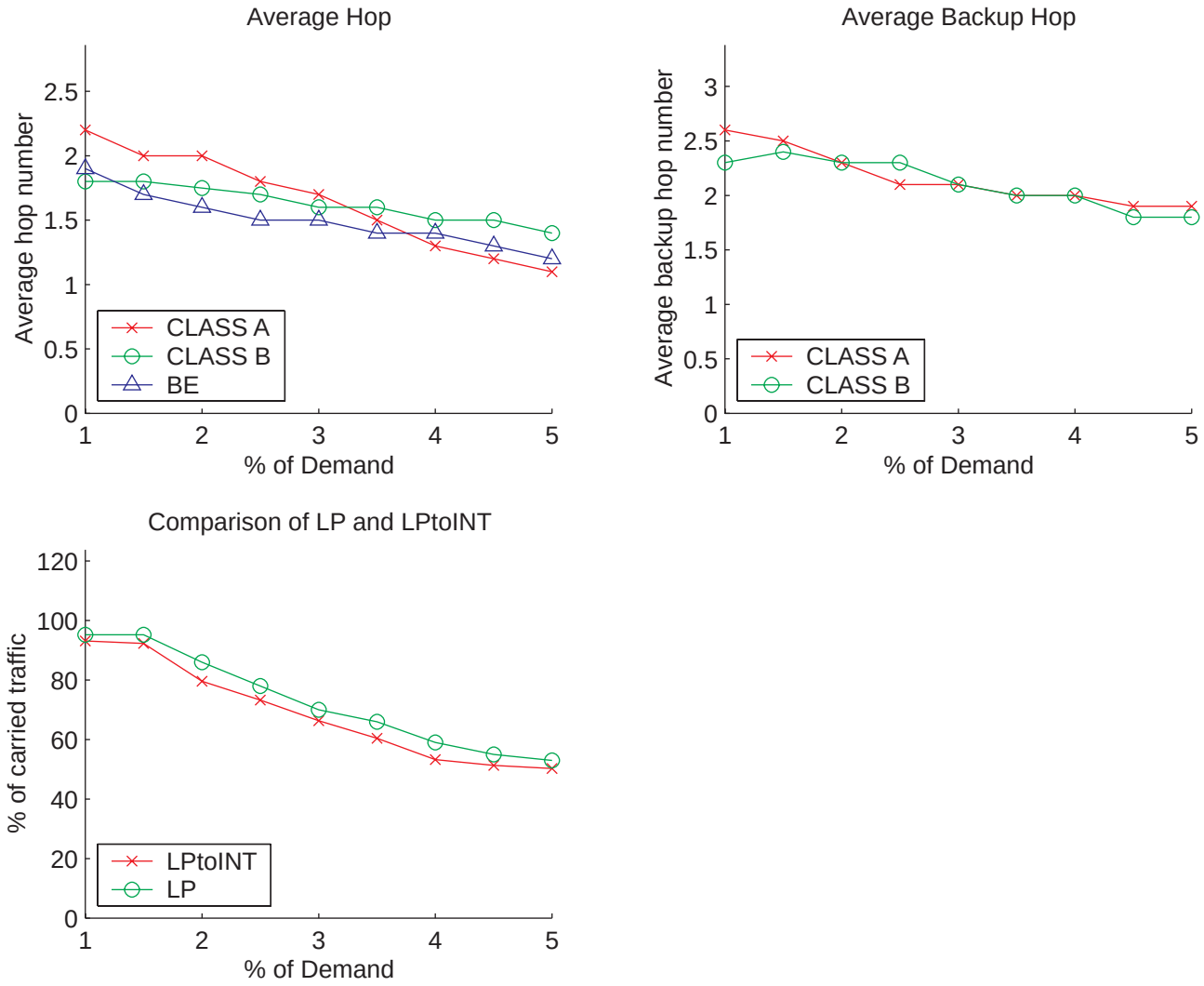

Figure 3.28: 1:1 link disjoint path protection with B_σ for Network 2

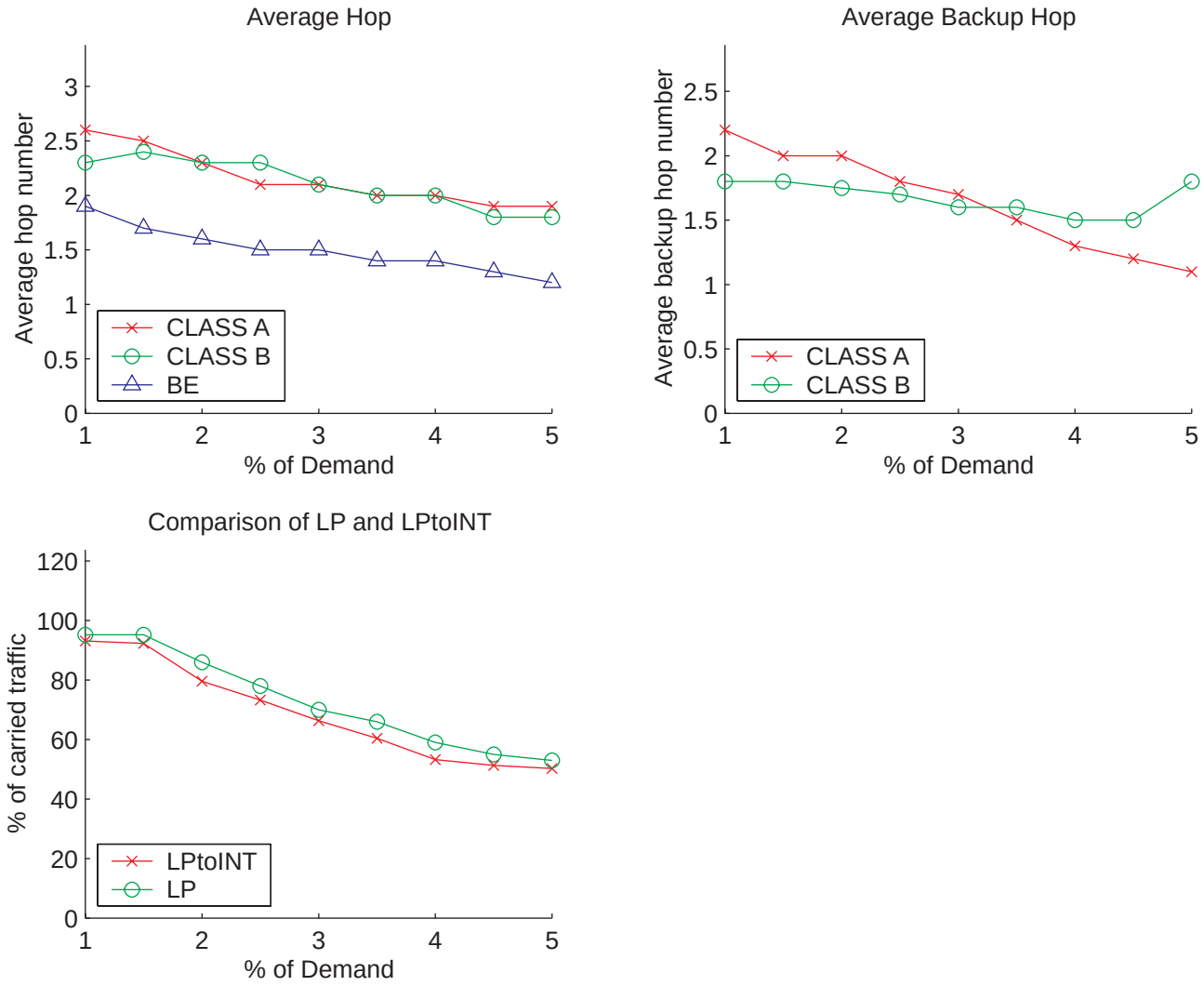

Figure 3.29: 1:1 link disjoint path protection without B_σ for Network 2

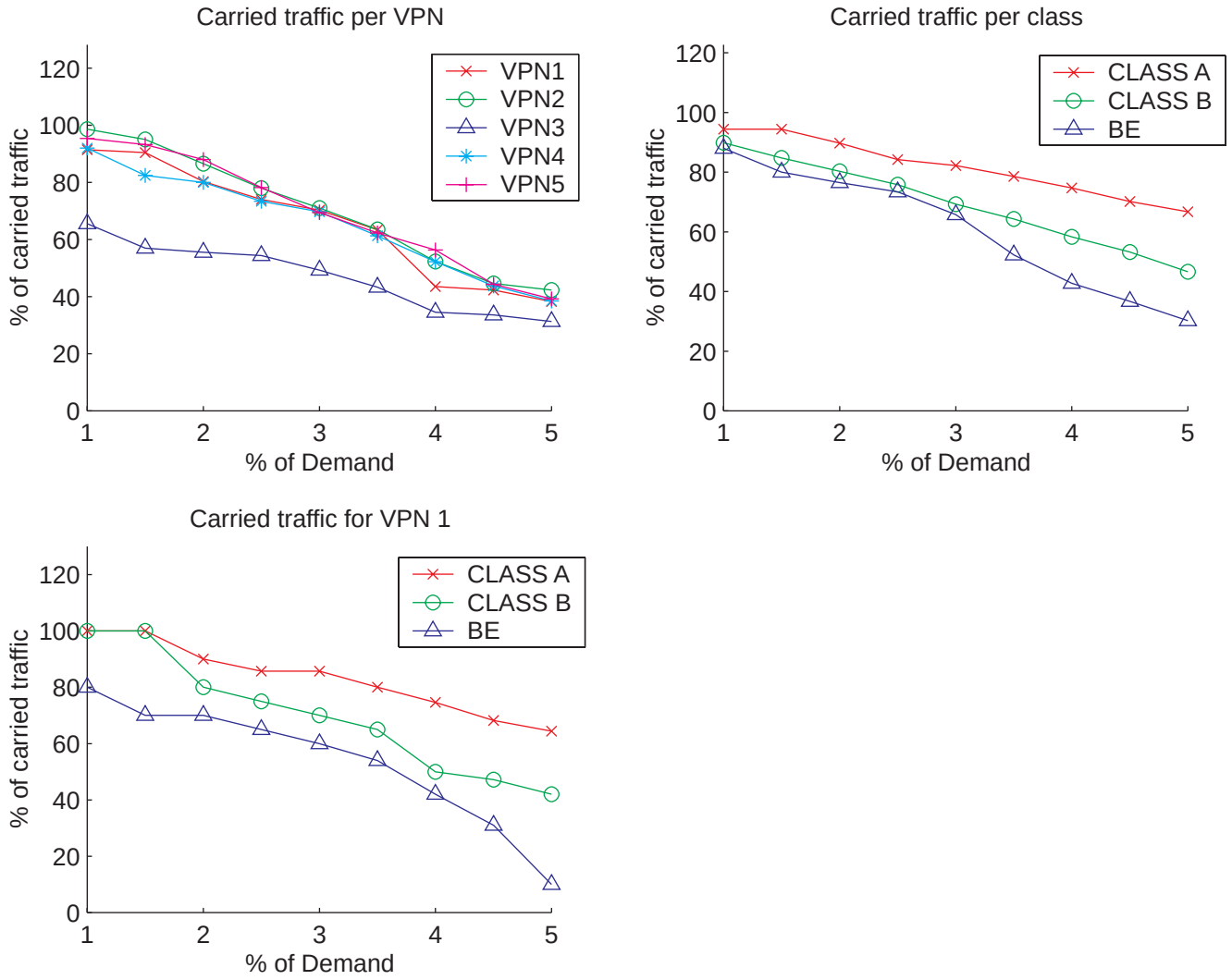

Figure 3.30: 1:1 link disjoint path protection with B_σ for Network 3

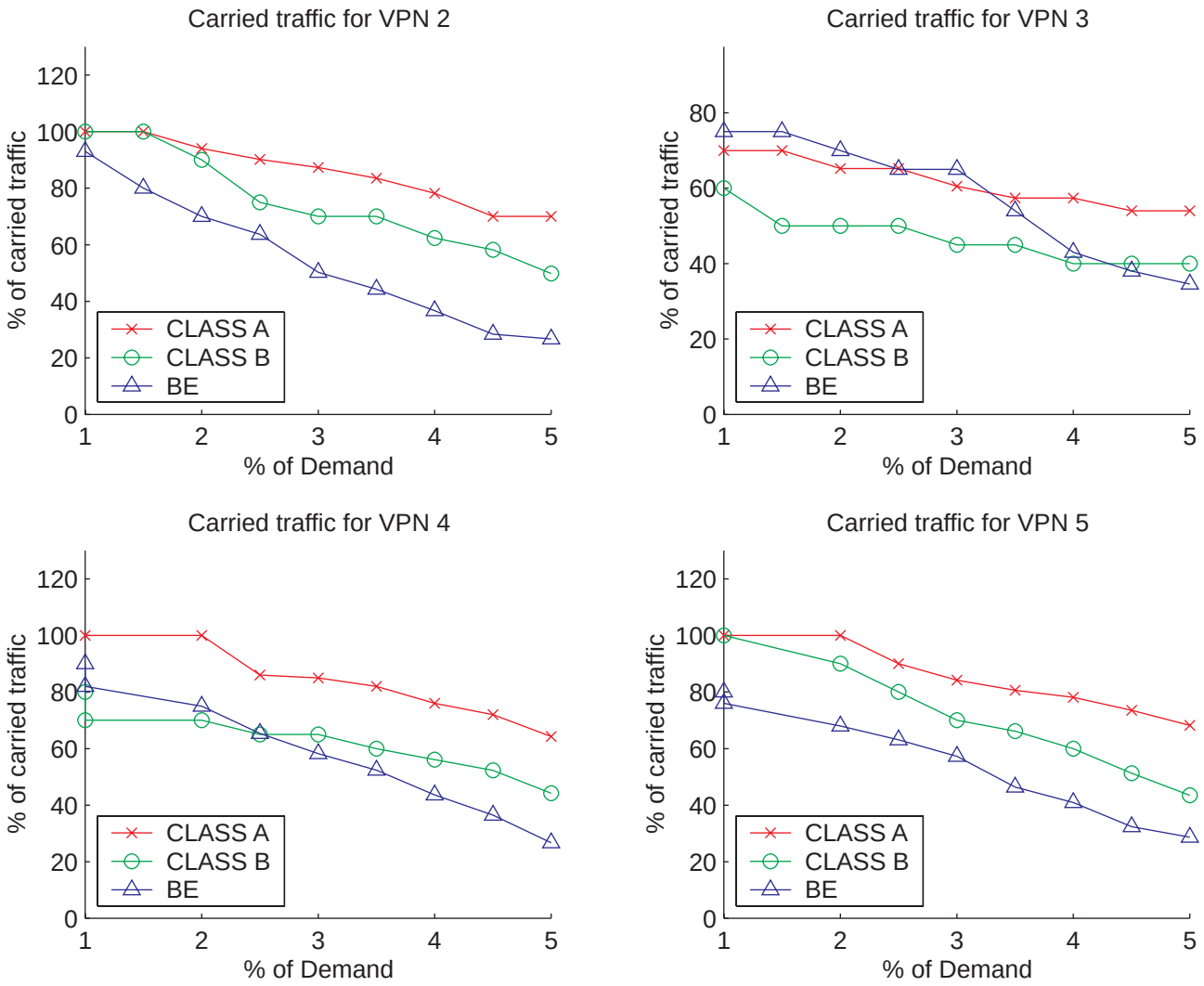

Figure 3.31: 1:1 link disjoint path protection with B_σ for Network 3

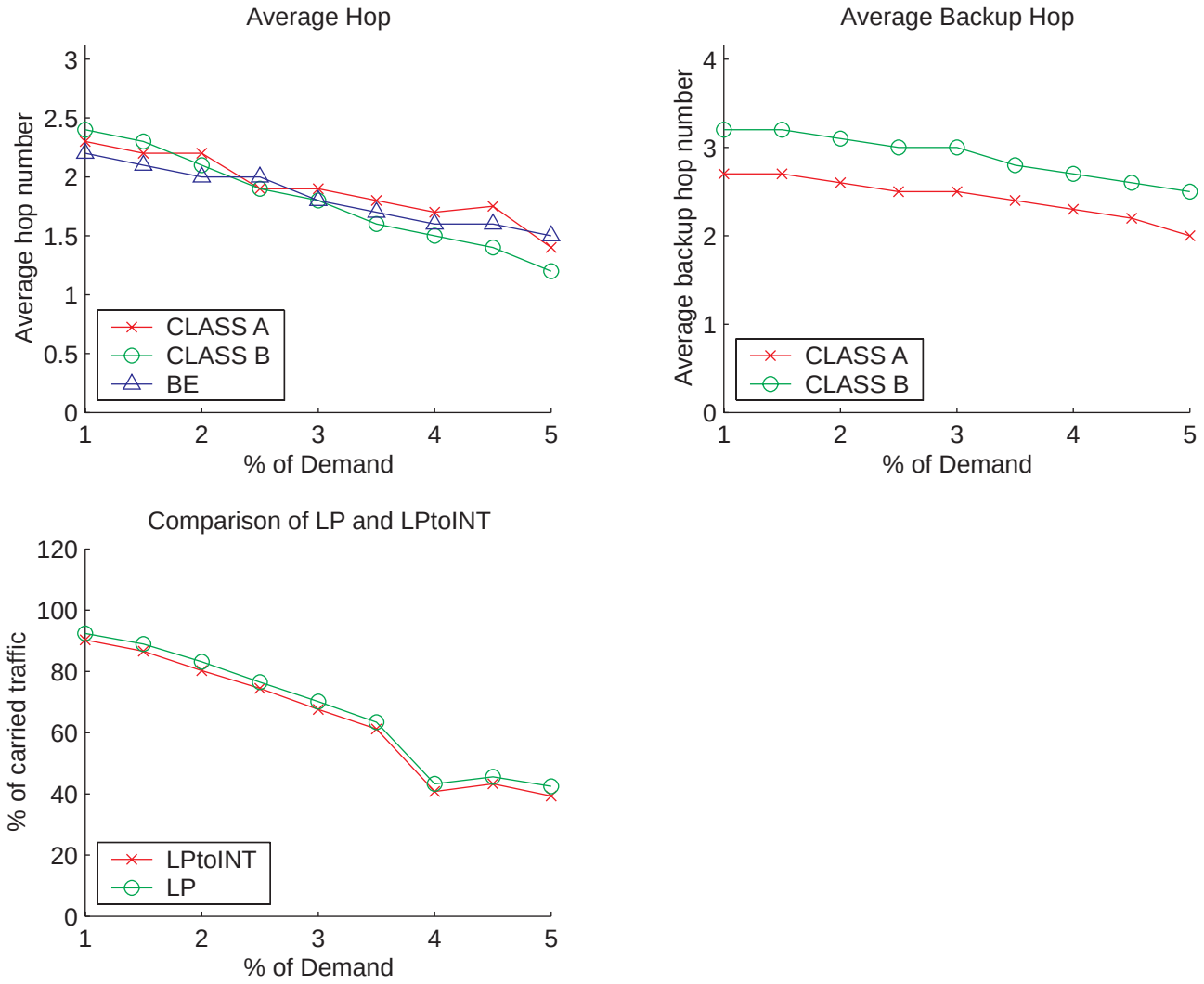

Figure 3.32: 1:1 link disjoint path protection with B_σ for Network 3

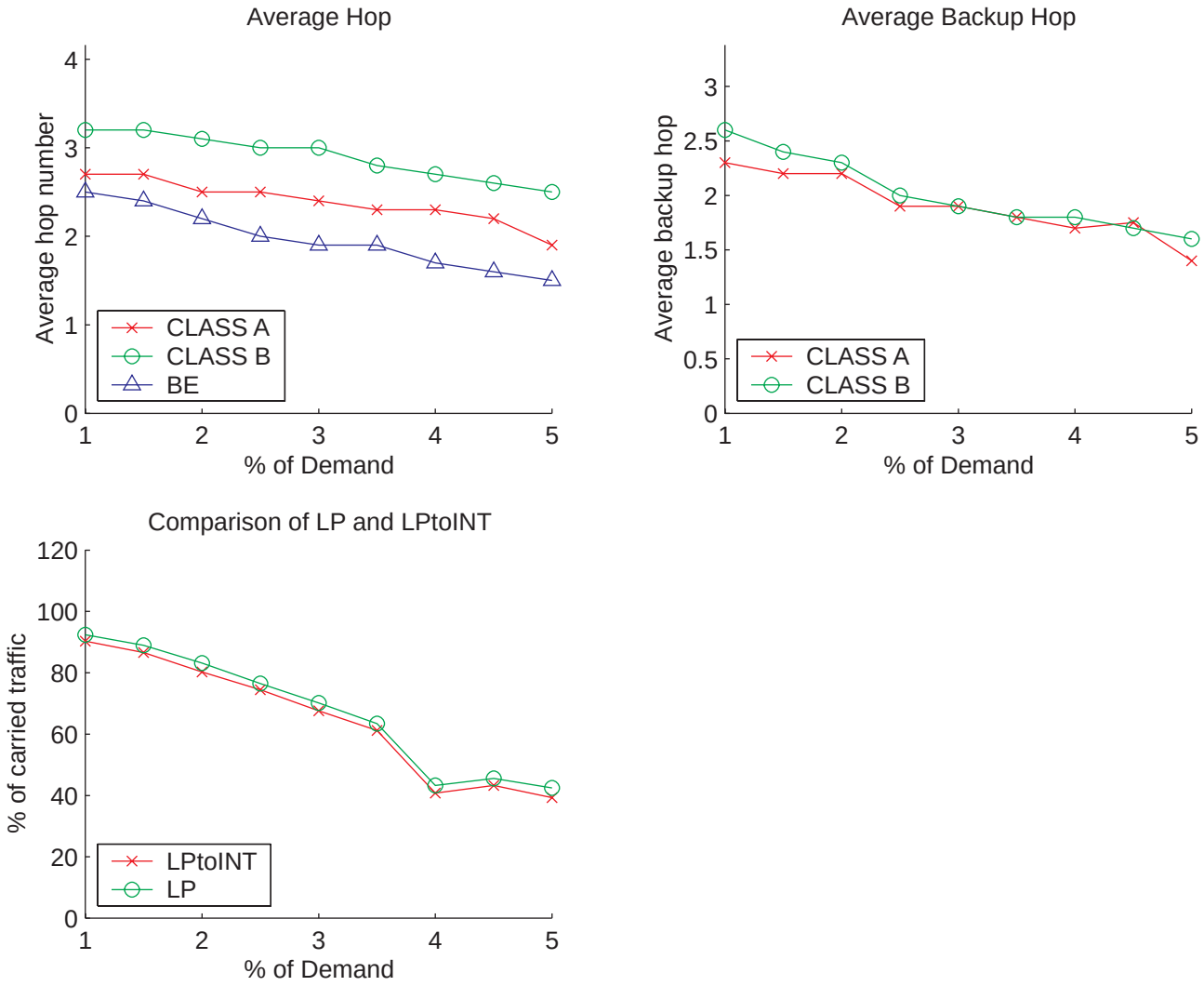

Figure 3.33: 1:1 link disjoint path protection without B_σ for Network 3

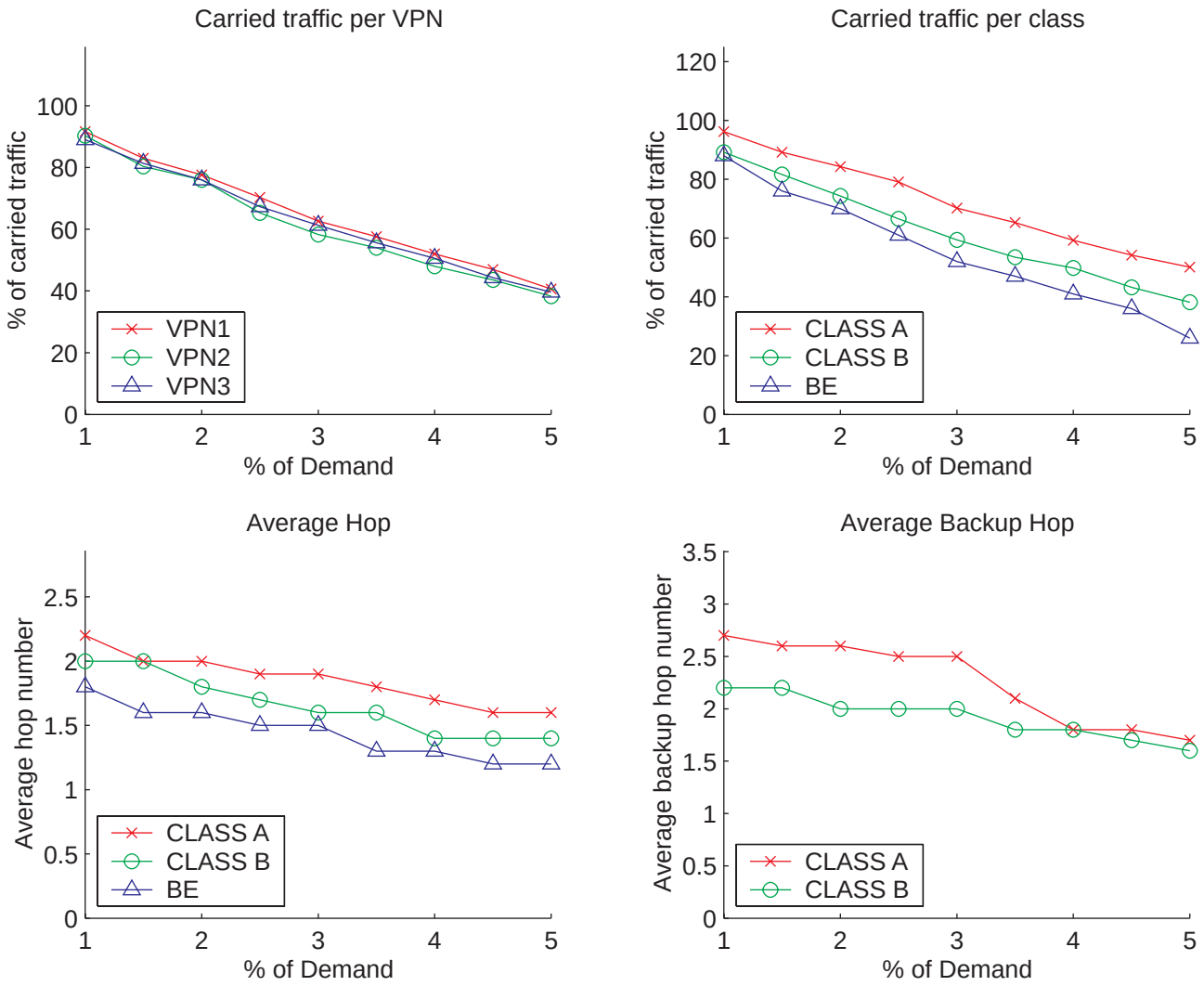

Figure 3.34: 1:1 node disjoint path protection with B_σ for Network 1

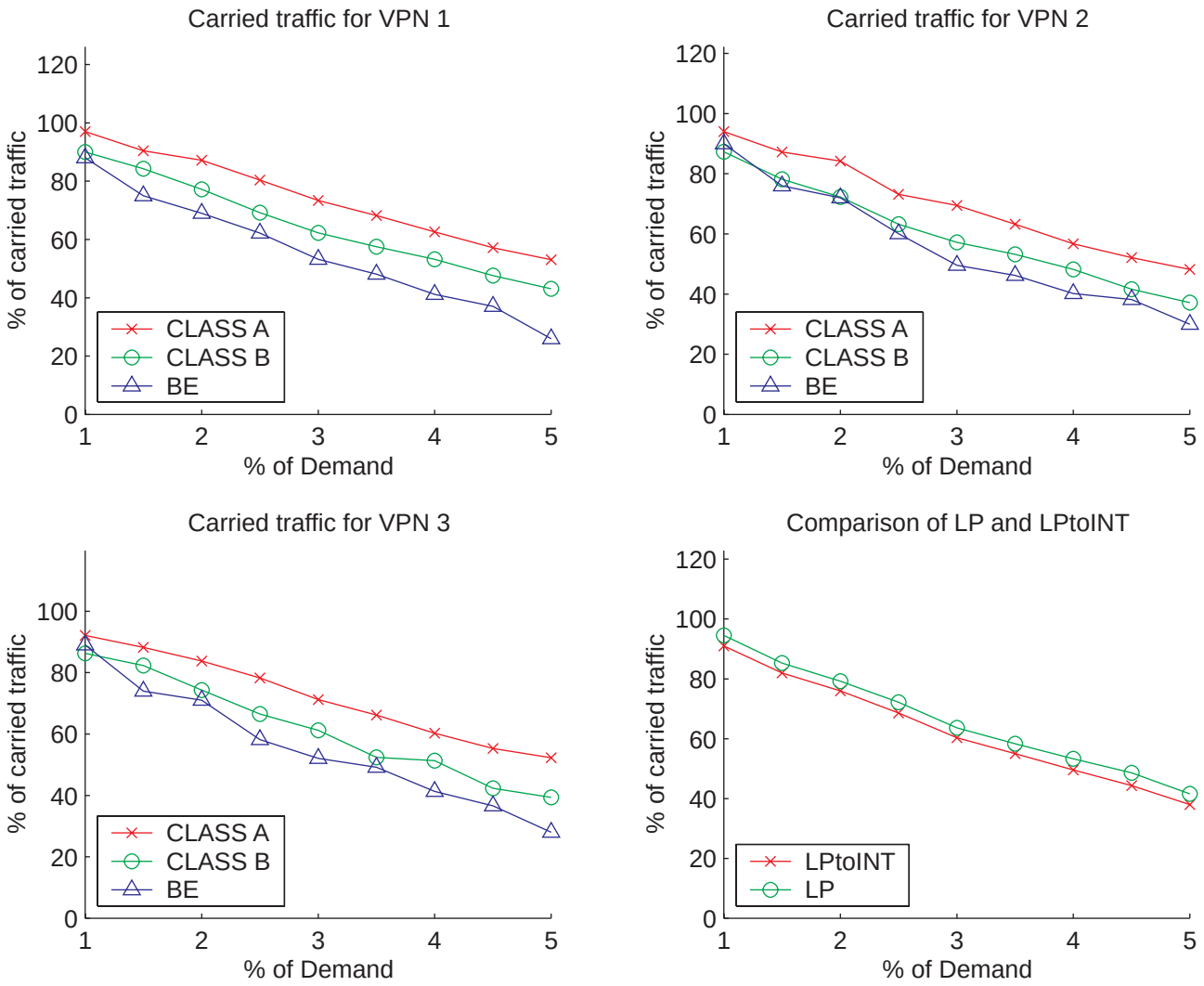

Figure 3.35: 1:1 node disjoint path protection with B_σ for Network 1

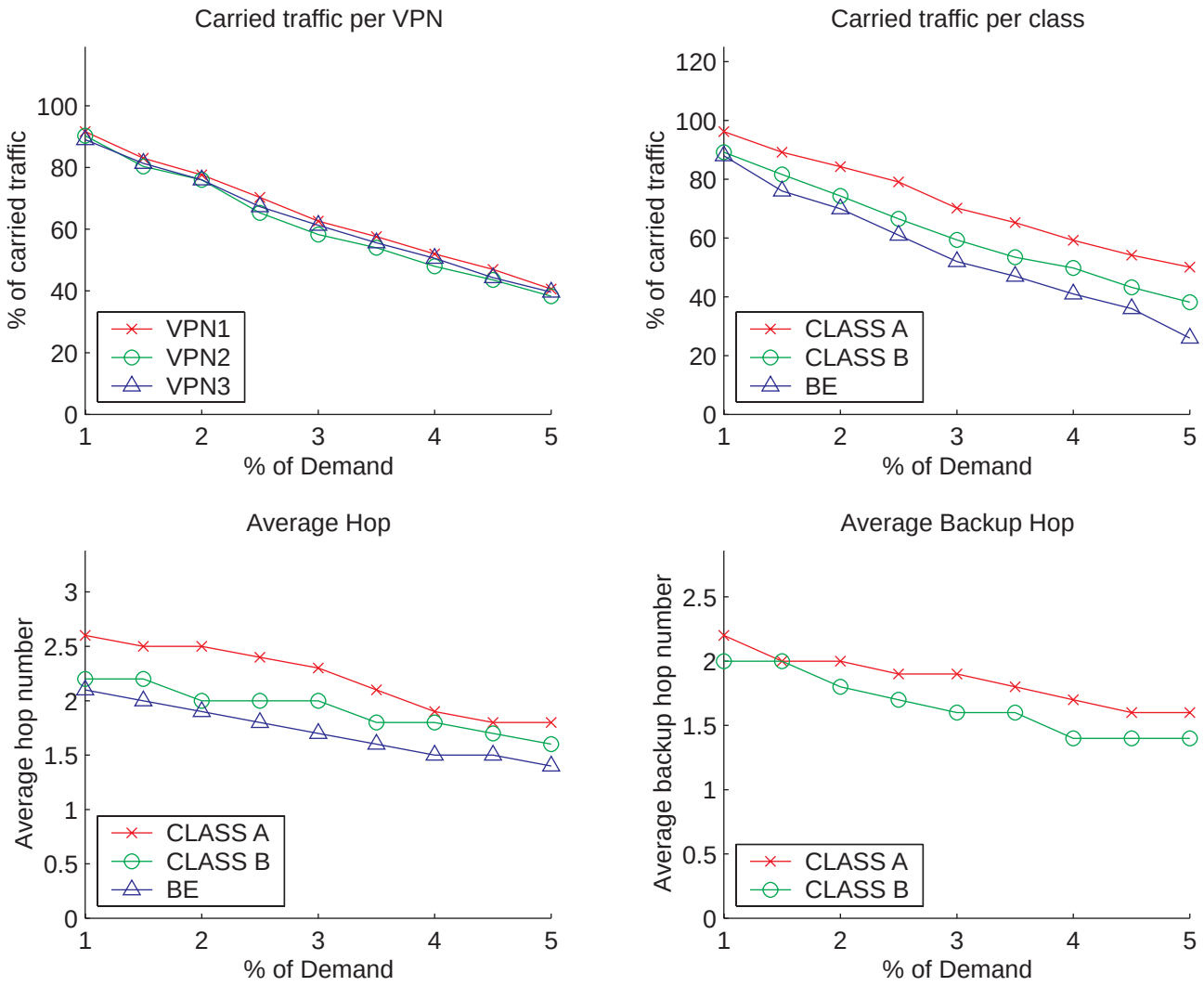

Figure 3.36: 1:1 node disjoint path protection without B_σ for Network 1

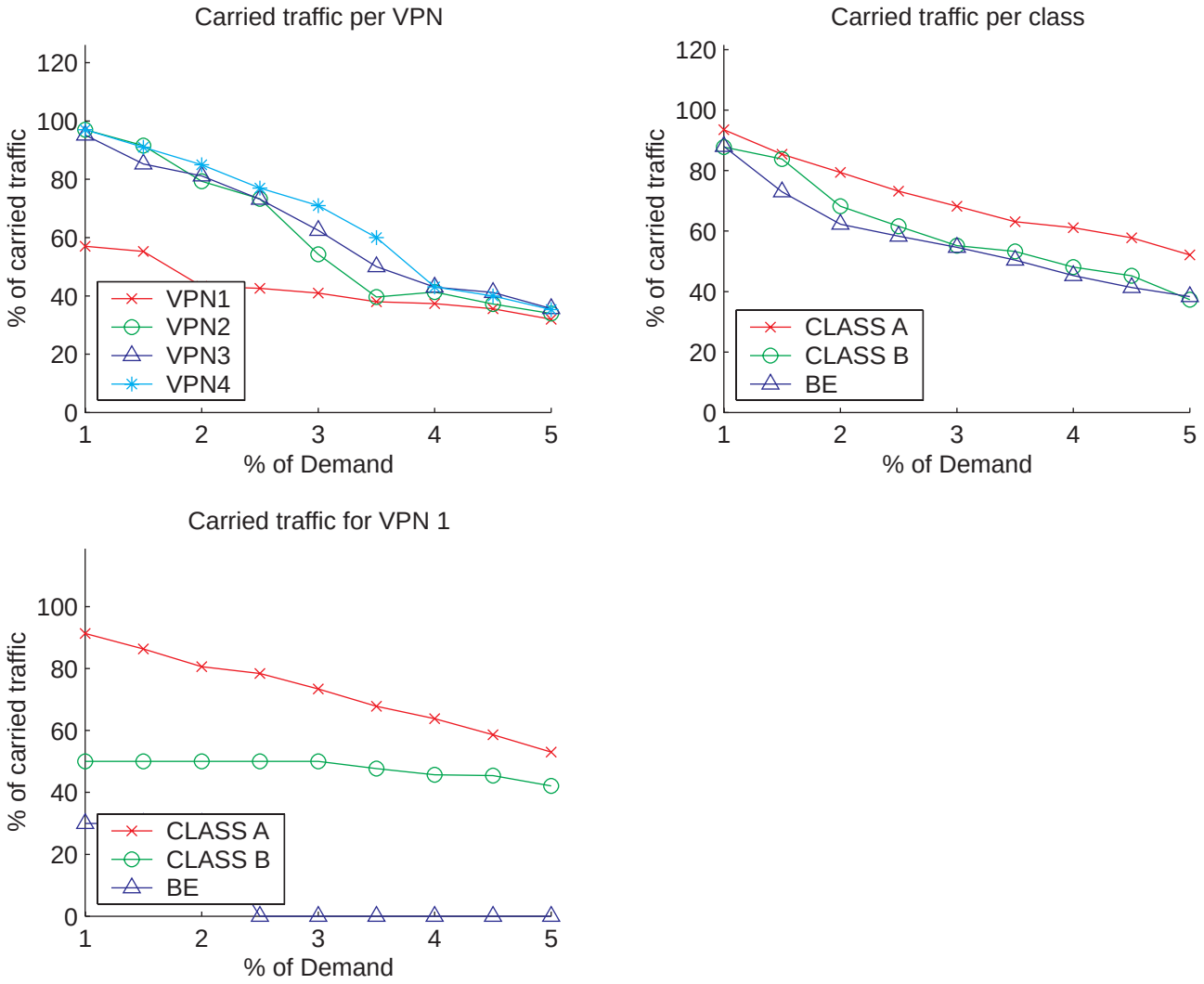

Figure 3.37: 1:1 node disjoint path protection with B_σ for Network 2

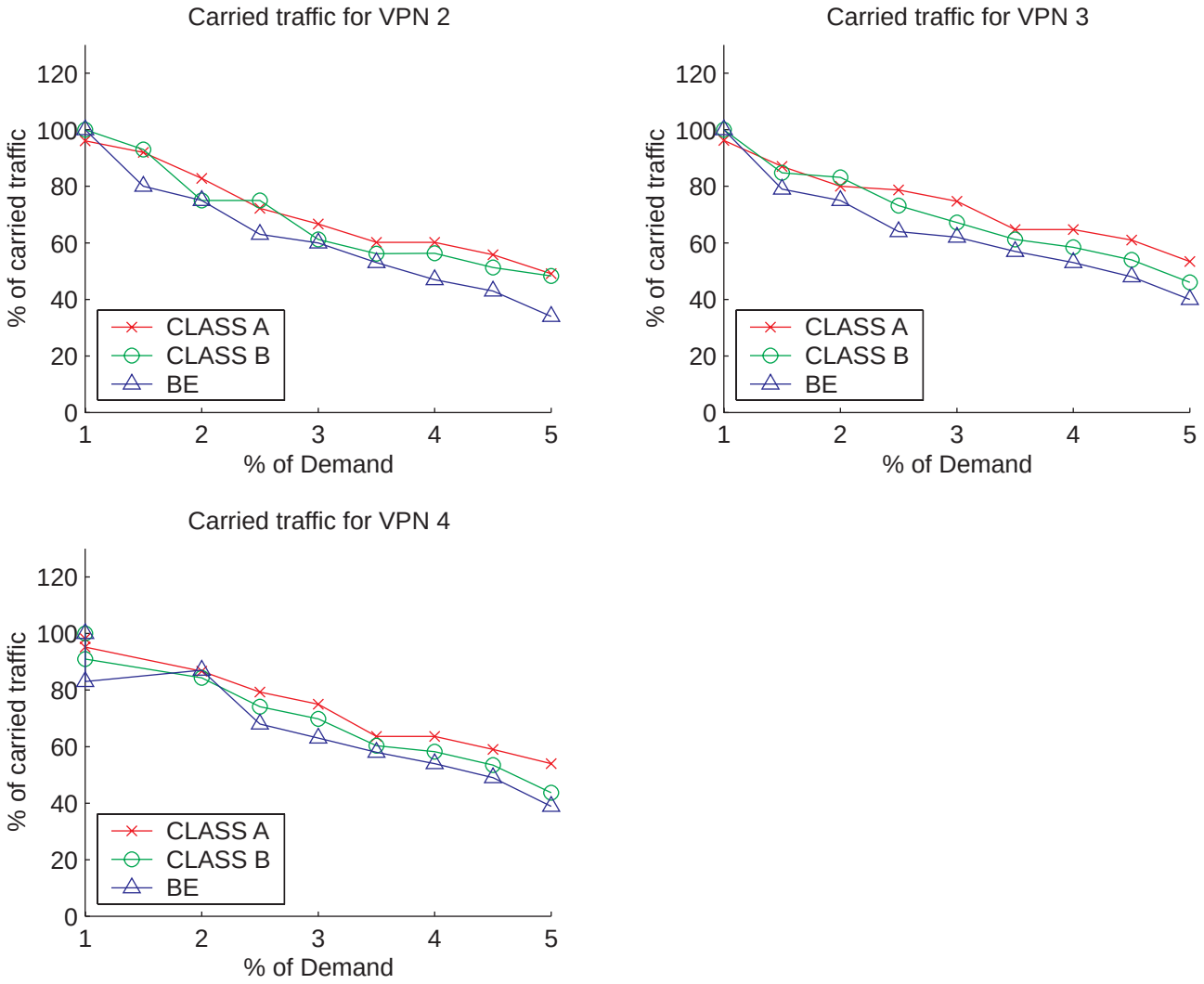

Figure 3.38: 1:1 node disjoint path protection with B_σ for Network 2

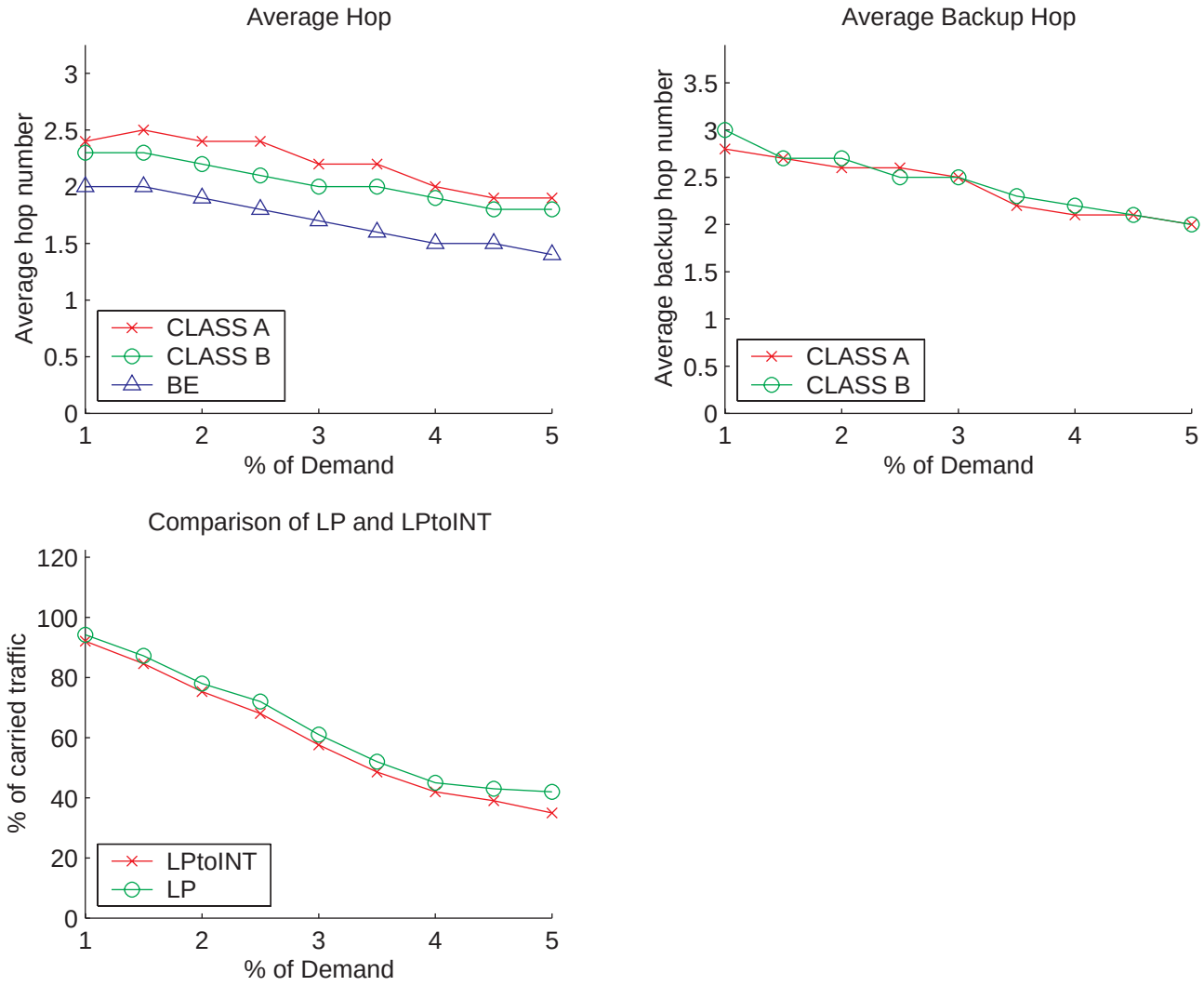

Figure 3.39: 1:1 node disjoint path protection with B_σ for Network 2

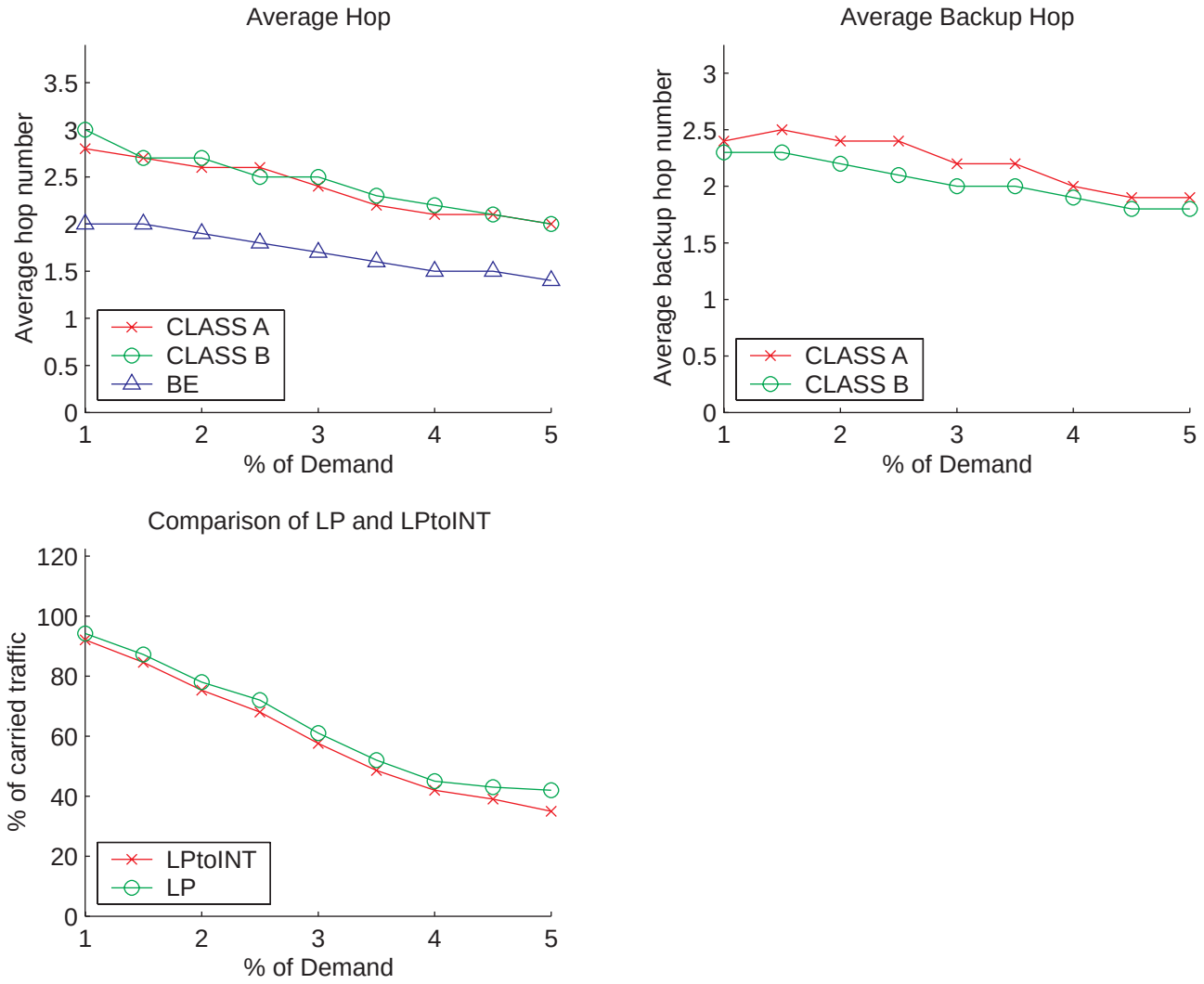

Figure 3.40: 1:1 node disjoint path protection without B_σ for Network 2

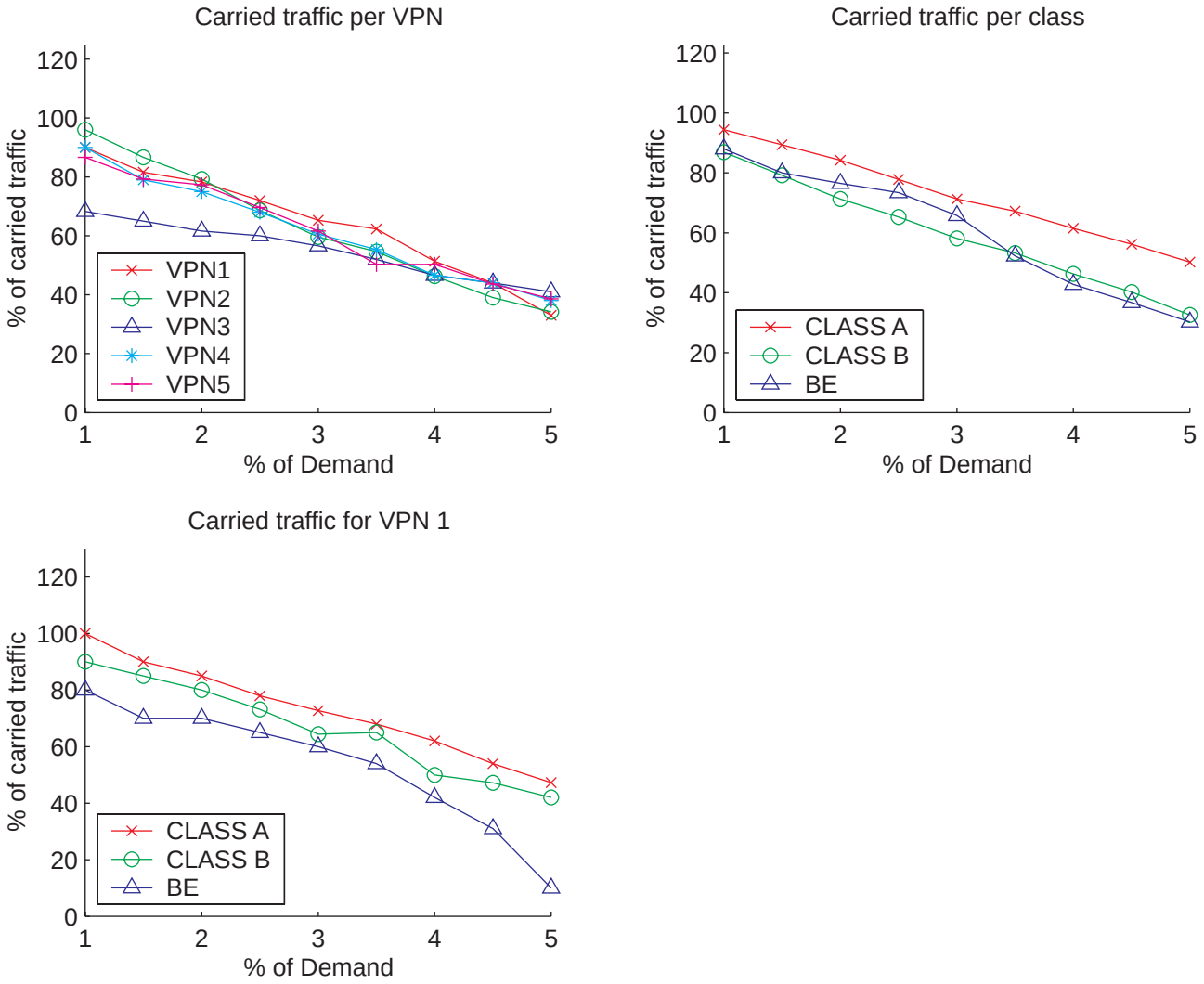

Figure 3.41: 1:1 node disjoint path protection with B_σ for Network 3

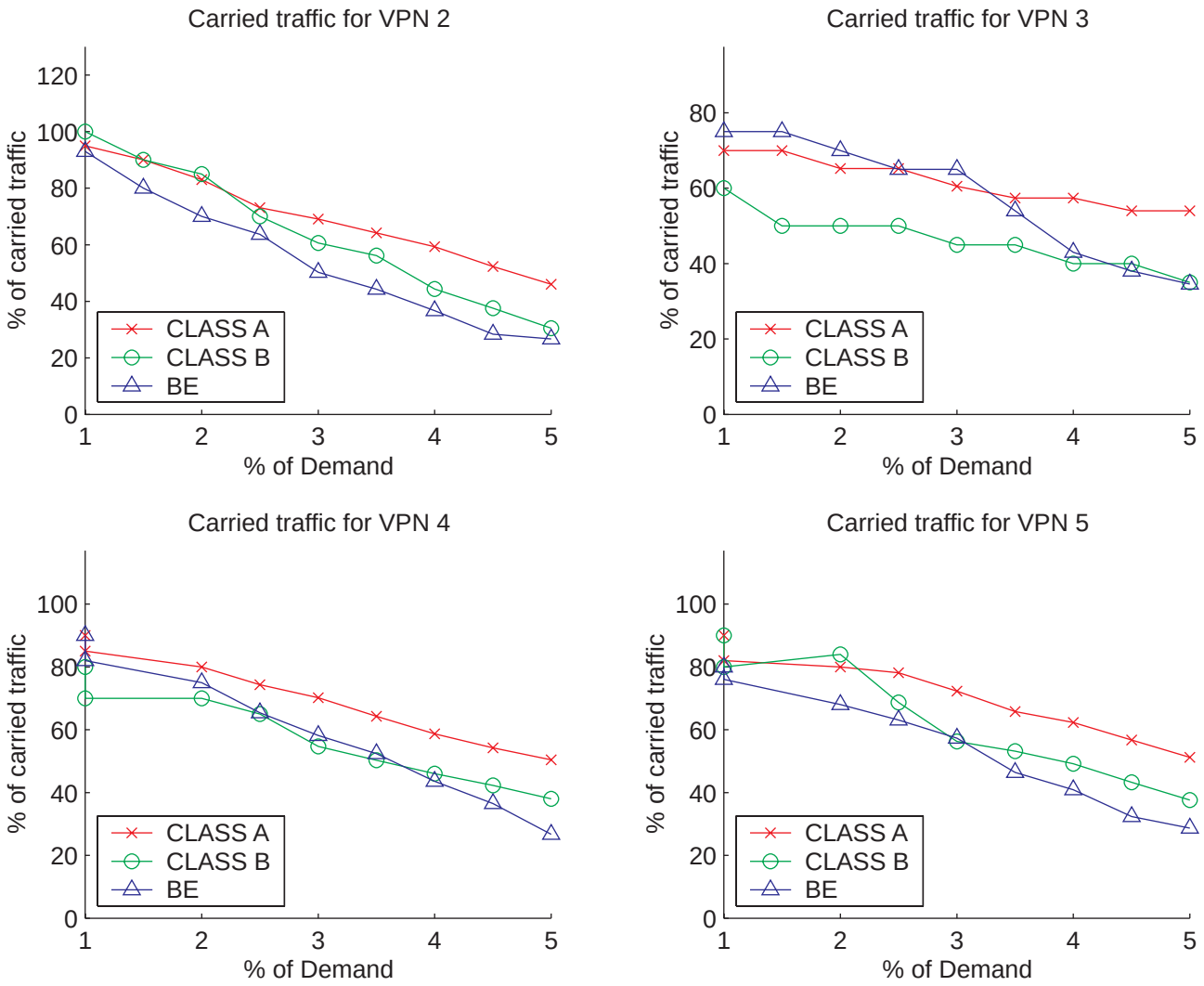

Figure 3.42: 1:1 node disjoint path protection with B_σ for Network 3

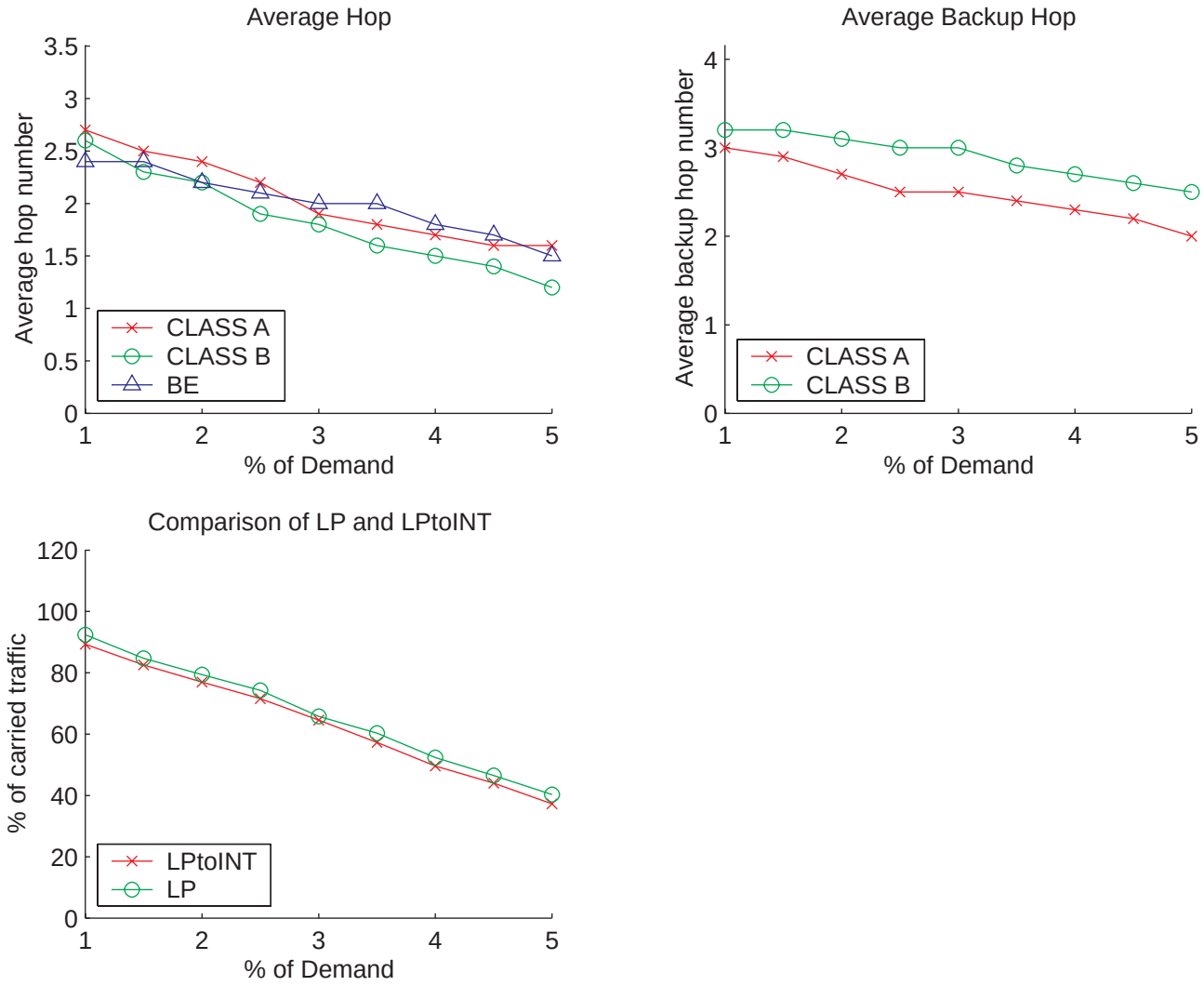

Figure 3.43: 1:1 node disjoint path protection with B_σ for Network 3

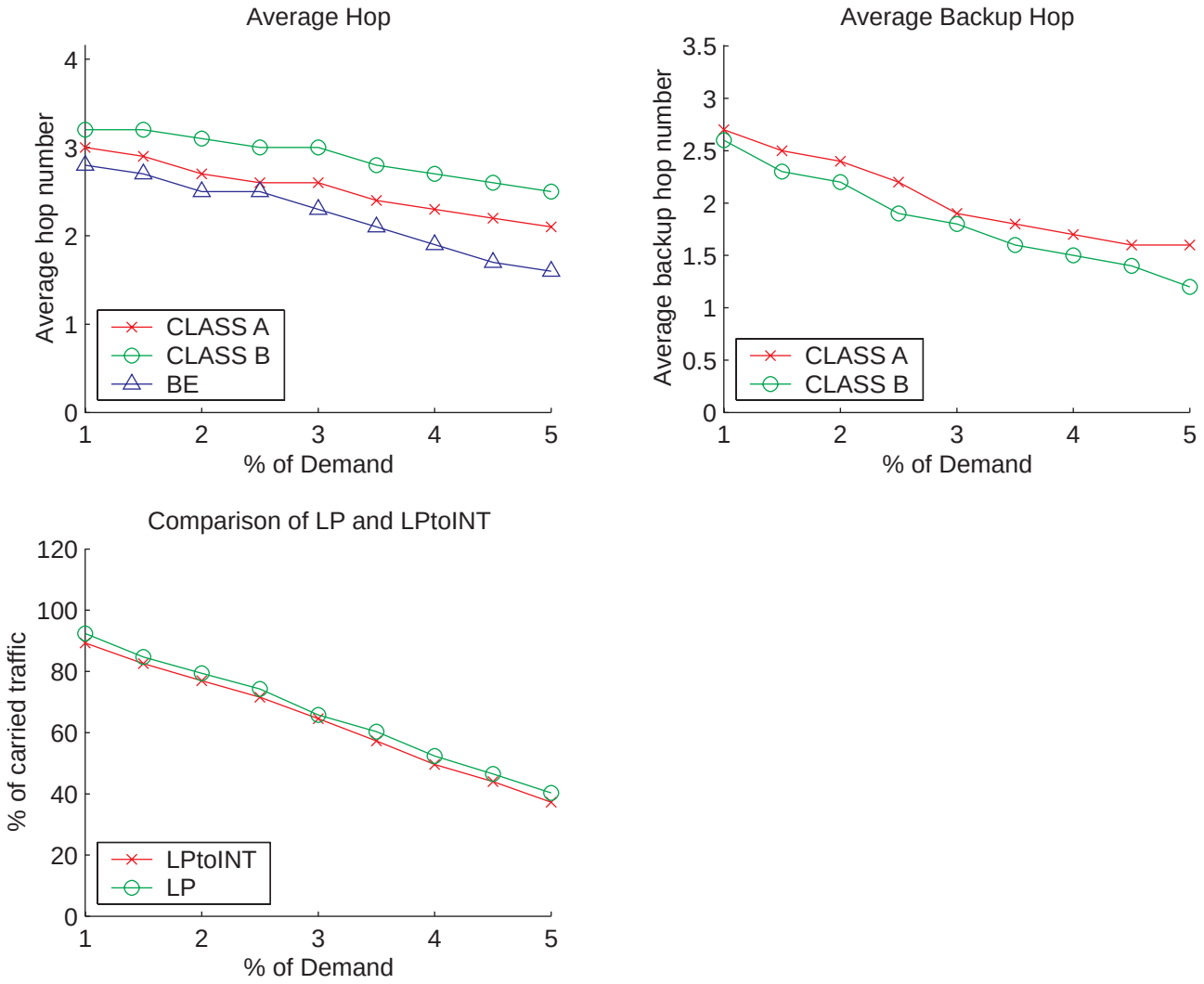

Figure 3.44: 1:1 node disjoint path protection without B_σ for Network 3

Chapter 4

Conclusion

In this thesis, we proposed several approaches to offline constraint-based routing algorithms for MPLS VPNs. We reviewed several algorithms from literature on MPLS network to extend the approach to VPNs. We implemented the route based and link based routing techniques for QoS and BE traffic. We modified the route based routing technique to accommodate MPLS VPN's. Thus, it is possible to specify certain admissible route sets for each OD pair and each class of traffic for each of the VPN's in the MPLS network. We modified the objective function to accommodate MPLS VPN's and also to account for utilization of network resources. We also modified the link based routing algorithm discussed in the literature to accommodate routing of QoS and BE traffic in MPLS VPN's. We also studied the effect of parameters such as epsilon, granularity and earning rate on traffic routed in the network. We implemented onestage and twostage routing of QoS and BE traffic to show the effect of different earning rates and priorities in the network. We also studied the effect of hop count on routing under light and heavy load conditions. Our algorithms also supported various path protection schemes such as $1+1$ and $1:1$ link disjoint and node disjoint for link based routing of QoS traffic. Our approach is scalable and can be employed to large number of VPNs as inferred from the results. The algorithms were simulated on three networks (US abstract network and two hierarchical synthetic networks). In order to overcome the computational complexity of solving MIP problems, we used the LP -to-Integer approach discussed in [4]. We also studied the comparison of the results obtained from the LP and LP-to-Integer approach.The approximation provides an optimal result as seen from the graphs.

Bibliography

[1] D.Mitra and K.G. Ramakrishnan, "A case study of multiservice multipriority traffic engineering design for data networks" , *IEEE GLOBECOM*, 1999, pp.1077-1083.

[2] Xipeng Xiao, Alan Hannan, Brook Bailey and Lionel Ni, "Traffic engineering with MPLS in the Internet", *IEEE Network Magazine*, pp.28-33,March 2000.

[3] D.Awduche, J.Malcolm, J.Agogbus, M.O'Dell and J.McManus, "Requirements for Traffic Engineering over MPLS" , *RFC 2701* , Sept. 1999.

[4] Chung-Yu Wei, "Traffic Engineering in MPLS Networks" , *Master's Thesis, December 2003*

[5] Chung Tung Chou, "Traffic Engineering for MPLS based Virtual Private Networks" , *hhtp://www.elsevier.com/locate/comnet, Oct 2003*

[6] David Applegate,Mikel Thorrup, "Load optimal MPLS Routing with N + M Labels" , *IEEE INFOCOM, 2002*

[7] Mort Naraghi-Pour and Manju V. Hedge, "Path Protection in MPLS Networks" , *Celox Networks, Inc* , November, 2001.

[8] M.K. Girish, Z. Bei, and J. Hu, "Formulation of the Traffic Engineering Problems in MPLS based IP Networks", *INFOCOM* , 2000.

[9] Manju Hegde, Mort Naraghi-Pour, "Engineering traffic in MPLS networks" , *http://www.eetimes.com/story/OEG20011121S0066*

[10] Y Wang,Z Wang, "Explicit Routing Algorithms for Internet Traffic Engineering" , *ICCCN,*1999.

[11] Youngseok Lee, Yongho Seok, Yanghee Choi and Changhoon Kim, "A Constrained Multipath Traffic Engineering Scheme for MPLS Networks" , *IEEE* , 2002, pp.2431-2436.

[12] E. W. Zegura, "GT-ITM: Georgia tech internetwork topology models (software)" , *http://www.cc.gatech.edu/fac/Ellen.Zegura/gt-itm/gt-itm.tar.gz* , 1996.

[13] ILOG CPLEX, *http://www.ilog.com/products/cplex/*

[14] Mort Naraghi-Pour and Manju V. Hedge, "Path Protection in MPLS Networks" , *Celox Networks, Inc* , November, 2001.

[15] M.K. Girish, Z. Bei, and J. Hu, "Formulation of the Traffic Engineering Problems in MPLS based IP Networks", *INFOCOM* , 2000.

[16] Changcheng Huang, Vishal Sharma, Ken Owens and Srnivas, "Building Reliable MPLS Networks Using a Path Protection Mechanism" , *IEEE Communications Magazine* , March 2002.

[17] Teunis Ott, Tony Bogovic, Tami Carpenter, K.R. Krishnan, and David Shallcross, "Algorithm for Flow Allocation for Multi Protocol Label Switching" , *Telcordia Technologies, Inc* , Auguest. 2000.

[18] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture" , *RFC 3031* , 2001.

[19] E. Rosen, Y. Rekhter "BGP/MPLS VPN's" , *RFC 2547*, 1999.

[20] *http://www.ixiacom.com.*

Vita

Pooja S Aniker is from Bangalore which is in the Southern part of India. She received her Bachelor of Engineering degree in Electronics and Communication from M.S. Ramaiah Institute of Technology,Bangalore University, Bangalore in 2001. She enrolled in the Department of Electrical and Computer Engineering at Louisiana State University, Baton Rouge, Louisiana, USA in the Fall of 2002 and will receive her Master of Science in Electrical Engineering degree majoring in communication in Spring 2005.