AMPLE Using IGP Based Traffic Engineering

Dr.V. Palanisamy [#1], K. Gowri [*2]

[#]*Department of Computer Science and Engineering, Alagappa University*
Karaikudi – 630004, Tamil Nadu, India
[*]*Department of Computer Science and Engineering, Alagappa University*
Karaikudi – 630004, Tamil Nadu, India

Abstract - **Literature survey is most important for understanding and gaining much more knowledge about specific area of a subject. In this paper survey on traffic engineering in IP networks. It provides a thorough analysis of the existent traffic engineering approaches. It's mainly used for handling traffic dynamics in order to avoid network congestion. In our proposal we introduce AMPLE (Adaptive Multi-toPoLogy traffic Engineering), this system based on virtualized IGP routing topologies for dynamic traffic engineering. The proposed system consists of two complementary Components: offline link weight optimization that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual routing topologies for long term operation through the optimized setting of link weights. Based on these diverse paths, adaptive traffic control performs intelligent traffic splitting across individual routing topologies in reaction to the monitored network dynamics at short timescale. A new proposal for achieving better quality of service and overall network performance in IP networks.**

Keywords - **Traffic Engineering, IGP, OSPF, IS-IS, AMPLE, OLWO, ATC.**

I. INTRODUCTION

A. *Network*:

A network consists of two or more computers that are linked together. In order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

There are many types of computer networks, they are listed below:

`Local-area networks (LANs)` **:** The computers are geographically close together (that is, in the same building).

`Wide-area networks (WANs)` : The computers are farther apart and are connected by telephone lines or radio waves.

`Campus-area networks (CANs):` The computers are within a limited geographic area, such as a campus or military base.

`Metropolitan-area networks (MANs):` A data network designed for a town or city.

`Home-area networks (HANs):` A network contained within a user's home that connects a person's digital devices.

B. *Network Security:*

Computer networks are widely used to connect computers at distant locations. Protecting vital information starts right at the edge of your network. Dealing with each attack is time-consuming and expensive.

Raises additional security problems:

- Data in transmission must be protected.
- Network connectivity exposes each computer to more vulnerabilities.

C. *Basic Security Requirements*

To provide adequate protection of network resources, the procedures and technologies that you deploy need to guarantee three things, sometimes referred to as the CIA triad:

`Confidentiality:` Providing confidentiality of data guarantees that only authorized users can view sensitive information.

`Integrity:` Providing integrity of data guarantees that only authorized users can change sensitive information and provides a way to detect whether data has been tampered with during transmission; this might also guarantee the authenticity of data.

`Availability of systems and data:` System and data availability provides uninterrupted access by authorized users to important computing resources and data.

Many network security threats today are spread over the Internet. The most common include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

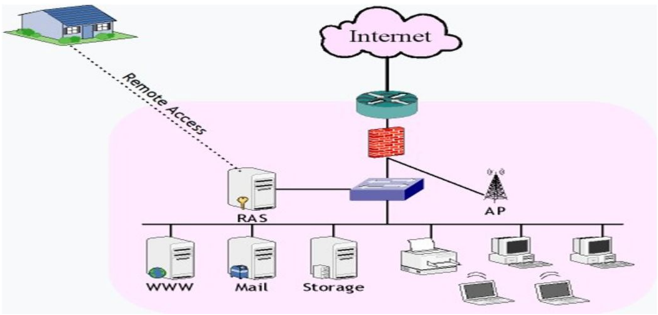

Fig. 1 Example of Network process

D. Networking security concepts:

The key to network security can be found in understanding the choices and strategies available to you look to the building blocks of network security. These include implementing user authentication, using proxy servers and firewalls, setting up demilitarized zones, and taking advantage of port- and packet-filtering technologies.

- Fundamental concepts in network security, including identification of common vulnerabilities and threats, and mitigation strategies
- Implementation of a security architecture using a lifecycle approach, including the phases of the process, their dependencies, and the importance of a sound security policy

II. RELATED WORK

A. Traffic Engineering Overview:

Traffic engineering by finding a suitable set of weights in OSPF/IS-IS is a well studied area of research and it is described in recent textbooks in the area [17, 15, and 16]. Traffic engineering is a method of optimizing the performance of a telecommunications network by dynamically analyzing, predicting and regulating the behavior of data transmitted over that network. It is an important mechanism for Internet network providers seeking to optimize network performance and traffic delivery [2]. Traffic engineering involves adapting the routing of traffic to the network conditions, with the joint goals of good user performance and efficient use of network resources. Most work on traffic engineering has focused on techniques for controlling the flow of traffic within a single Autonomous System (AS), such as a company, university campus, or Internet Service Provider (ISP). TE has been considered as one of the vital components of an autonomous system required to achieve both high resource utilization and high quality of service for both real time and non real-time applications [14, 13].

Congestion in the network causes poor throughput and long delays for end users, and also leads to an inefficient usage of network resources. In the Internet today, end users run the Transmission Control Protocol (TCP) to adapt their sending rates to congestion. Independently, Internet Service Providers (ISPs) monitor their networks for signs of overloaded links and adapt routing to alleviate congestion in a process known as traffic engineering (TE). The current state of the art for TE occurs at the timescale of hours and is centralized [22, 21, 20].

B. Traffic Measurements:

1) Connectionless Traffic Engineering

Connectionless is IP based approach. Connectionless traffic engineering model counts on traditional Interior Gateway Protocols (IGP), such as OSPF (Open Shortest Path First) and IS-IS (Intermediate System-Intermediate system). OSPF and IS-IS are basically link state protocols based on a shortest path algorithm. They develop and maintain a full knowledge of network routers, as well as how they interconnect [6].

2) Connection-oriented Traffic Engineering

Connection oriented is signaled based approach. The connection–oriented approach of traffic engineering refers basically to Multi-Protocol Label Switching (MPLS) [6].

In existing system, the traffic engineering is based in Interior Gateway Protocols (IGPs) that works within autonomous system. Such as Open Shortest Path First (OSPF) and Intermediate System-Intermediate System (IS-IS).

C. Traffic Engineering Framework

In this section, we formalize an approach to traffic engineering based on external changes in the IGP configuration. Assigning link weights based on the traffic demands and performance objectives depends on several key ingredients, as illustrated in Figure 2. First, instrumentation of the operational network should provide information about the status of the network elements and the current offered traffic. In practice, this topology and traffic data are necessary for a variety of other operational tasks. Second, evaluating possible settings of the link weights depends on having an accurate model of how the IGP configuration affects the flow of traffic. Third, selecting good settings of the weights depends on having an objective function that captures the key performance and reliability constraints, as well as an efficient algorithm for computing weights that satisfy these constraints; we discuss these optimization issues in more detail in Section 3. Fourth, after deciding on the values of the weights, an automated system or a human operator needs to effect these changes in the operational network [1].

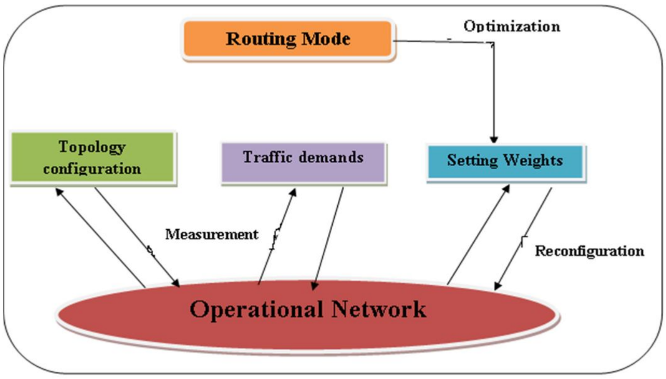

Fig. 2 Example of TE Framework

D. Traffic Engineering Objectives:

- Minimization of packet loss
- Minimization of delay
- Maximization of throughput
- Enforcements of service level agreements

III. LITERATURE OF BACKGROUND:

In literature survey, multi-topology IGP (MT-IGP) based intra-domain traffic engineering (TE) scheme. It is able to handle traffic problems, unexpected traffic fluctuations within the autonomous system. These are most useful for avoiding network congestion in effective manner.

A. Intra domain IGRP- Interior Gateway Routing Protocol:

The Interior Gateway Routing Protocol (IGRP) is an advanced distance vector routing protocol. The Interior Gateway Routing Protocol (IGRP) is a routing protocol that was developed in the mid-1980s by Cisco Systems, Inc. Cisco's principal goal in creating IGRP was to provide a robust protocol for routing within an autonomous system (AS). Such protocols are known as Interior Gateway Routing Protocols. An interior gateway protocol (IGP) is a routing protocol that is used to exchange routing information within an autonomous system (AS).

Two types of IGP are under the link-state routing protocols are:

- ❖ Open Shortest Path First (OSPF)
- ❖ Intermediate System to Intermediate System (IS-IS).

Link State indicates that a router executing OSPF will be concerned with tracking the operational state of each of its network interfaces. A change in the operational state of an interface is what triggers the router to send a routing update. This is in stark contrast to RIP, which is a timer-based protocol that sends routing updates every 30 seconds, whether or not changes in the network have occurred.

B. Traffic Engineering in OSPF networks:

In this section, a network model will be presented. Based on the network model, some fundamentals of traffic engineering (TE) will be introduced, which include the commonly used cost and objective functions for quantitatively evaluating and comparing different TE methods [18]. Open Shortest Path First (OSPF) is the most commonly used intra-domain internet routing protocol. Traffic flow is routed along shortest paths, splitting flow at nodes where several outgoing links are on shortest paths to the destination. The weights of the links, and thereby the shortest path routes, can be changed by the network operator. The weights could be set proportional to their physical distances, but often the main goal is to avoid congestion, i.e. overloading of links, and the standard heuristic recommended by Cisco is to make the weight of a link inversely proportional to its capacity [4]. The IS-IS protocol is specified in ISO 10589. Each Intermediate System (IS) (router) advertises one or more IS-IS Link State Protocol Data Units (LSPs) with routing information. The Intermediate System to Intermediate System (IS-IS) protocol to support Traffic Engineering (TE) [8].

Shortest Path First (SPF) or link-state protocols such as Open Shortest Path First (OSPF) [12, 9] or Intermediate System-Intermediate System (IS-IS) [12, 10] are the most commonly used intra-domain internet routing protocols today. Traffic is routed along shortest paths to the destination. The weights of the links, and thereby the shortest path routes, can be changed by the network operator [11].

The main advantage of link state routing (OSPF) is that complete knowledge of topology allows routers to calculate routes that satisfy the incoming request. This can be useful for traffic engineering purposes where routes can be manipulated to meet different service requirements.

The OSPF routing protocol to support Quality- of-Service (QoS) routing in IP networks. Support for QoS routing can be viewed as consisting of three major components:

1. Obtain the information needed to compute QoS paths and select a path capable of meeting the QoS requirements of a given request,

2. Establish the path selected to accommodate a new request,

3. Maintain the path assigned for use by a given request [25].

IV. PERFORMANCE PROPERTIES

In this section, we discuss how we can engineer the flow of traffic using the traditional OSPF/IS-IS routing protocols in large networks, using an optimization algorithm to identify good IGP weight settings. First, we describe how to use objective functions to judge the quality of a particular solution to the routing problem. Next, we evaluate several heuristics for setting the link weights for a given topology and traffic matrix.
Drawing on the experiments in [1, 4], we show that good settings of the IGP weights perform within a few percent of an optimal distribution of traffic for realistic topologies and traffic demands. Then, we consider how to deal with fluctuations in the traffic demands over time without modifying the IGP weights and describe how to change the flow of traffic in the network with small modifications to the link weights. These results draw on the results of experiments in [12]. Readers interested in the results of experiments on a wide variety of real and synthetic topologies can refer to [27].

A. IS-IS:

The IS-IS (Intermediate System to Intermediate System)routing protocol has become increasingly popular, with widespread usage among Service Providers. It is a link state protocol, which enables very fast convergence with large scalability. It is also a very flexible protocol and has been extended to incorporate leading edge features such as MPLS Traffic Engineering.

The IS-IS routing protocol is a link-state protocol, as opposed to distance-vector protocols such as Interior Gateway Routing Protocol (IGRP) and Routing Information Protocol (RIP). Link-state offers several advantages over distance-vector protocols. It is faster converging, supports much larger internetworks, and is less susceptible to routing loops. Features of IS-IS included:

- Hierarchical routing
- Classless behavior
- Rapid flooding of new information
- Fast Convergence
- Very scalable
- Flexible timer tuning

B. Types of routing algorithms

The routing algorithms are classified into different types.

- Static or Dynamic
- Single-path or Multipath
- Flat or Hierarchical
- Host-intelligent or Router-Intelligent
- Intra-domain or Inter-domain
- Link State or Distance Vector

1) Static or Dynamic:

Static routing algorithms are hardly algorithms at all. Static routing table mapping are established by the network administrator prior to the beginning of routing [28]. They do not change unless the network administrator changes them. Algorithms that use static routes are simple to design and work well in environments. Where network traffic is relatively predictable and network design is relatively simple. Because static routing system cannot react to network changes, they are generally considered unsuitable for today’s large, constantly changing networks. Most of the dominant routing algorithms in the 1990s are dynamic.

Dynamic routing algorithms adjust, in real time, to changing network circumstances. They do this by analyzing incoming routing update messages. If the message indicates that a network changes has occurred, the routing software recalculates routes and sends out new routing update messages. These messages permeate the network, simulating routers to return their algorithms and change the routing tables accordingly.

Dynamic routing algorithms may be supplemented with static routes where appropriate [29]. For example, a router of last resort (a router to which all un routable packets are sent) may be designated. This router act as a repository for all un-routable packets, ensuring that all messages are at least handled in some way.

2) Single-Path or Multipath

Some sophisticated routing protocols support multiple paths to the same destination. These multipath algorithms permit traffic multiplexing over multiple lines; single path algorithms do not [30]. The advantages of multipath algorithms are obvious; they can provide substantially better throughput and reliability.

3) Flat or Hierarchical

Some routing algorithms operate in a flat space, while others using routing hierarchies. In a flat routing system, all routers are peers of all others. In a hierarchical routing system, some routers from what amounts to a routing backbone packets from non-backbone routers travel to the backbone routers, where they are sent through the backbone until they reach the general area of the destination. At this point, they travel from the last backbone routers through one or more non-backbone routers to the final destination.

Routing system often designate logical groups of nodes called domain autonomous, systems or areas. In hierarchical systems, some routers in a domain communicate with routers in other domains, while others can only communicate routers within their domain. In very large networks, additional hierarchical levels may exist. Routers at the highest hierarchical levels form the routing backbone [10].

Primary advantage of hierarchical routing is that it mimics the organization of most companies and therefore supports their traffic patterns very well. Most network communication occurs within small company groups (domains). Intra domain routers only need to know about other routers within their domain, so their routing algorithms can be simplified. Depending on the routing algorithm being used, routing updates traffic can be reduced accordingly [35].

4) Host-intelligent or Router-Intelligent

Some routing algorithms assume that the source end-code will determine the entire route. This is usually referred to as source routing, in source routing system, routers merely act as store-and-forward devices. Mindlessly sending the packet to the next stop.

Other algorithm assumes that hosts know nothing about routes. In these algorithms, routers determine the path through the internetwork based on their own calculations. In this first system, the hosts have the routing intelligence. In the latter system, routers have the routing intelligence. The trade-off between host intelligence and router intelligence is one of path optimality versus traffic overhead. Intelligence system chooses the better routes more often, because they typically discover all possible routes to the destination before the packet is actually sent. They when choose the path based on that particular system's definition of optimal. The act of determining all routes [31], however, often require substantial discovery traffic and significant amount of time.

5) Intra-domain or inter-domain

Some routing algorithms work only within domain; others work within and between domains. The natures of these two algorithms type are different. It stands to reason, therefore, that an optimal intra-domain routing algorithm would not necessarily be an optimal inter-domain routing algorithm.

6) Link state or distance vector

Link state algorithm (also known as *Shortest Path First* algorithms) flood routing information to all nodes in the internetwork. However each router sends only that portion of the routing table that describes the state of its own links.

Distance vector algorithms (also known as *Bellman-Ford* algorithms) [32] call for each router to send all or some portion of its routing table, but only to its neighbors. In essence, link state algorithms send small update everywhere, while distance vector algorithms send larger updates only to neighboring routers.

Because the coverage more quickly, link state algorithms are somewhat less prone to routing loops than distance vector algorithms. On the other hand, link state algorithms require more CPU power and memory than distance vector algorithms. Link state algorithms [34] can therefore be more expensive to implement and support. Despite their differences, both algorithm types perform well in most circumstances.

V. AMPLE:

AMPLE encompasses two distinct tasks, namely (1) offline network dimensioning through link weight optimization for achieving maximum intra-domain path diversity across multiple MT-IGP routing topologies; and (2) adaptive traffic splitting ratio adjustment across these routing topologies for achieving dynamic load balancing in case of unexpected traffic dynamics..*AMPLE* (Adaptive Multi-toPoLogy traffic Engineering), a current IGP TE approach that is capable of adaptively handling traffic dynamics in operational IP networks. Instead of re-assigning IGP link weights in response to traffic fluctuations, we adopt multi-topology IGPs (MT-IGPs) such as MT-OSPF and M-ISIS as the underlying routing platform to enable path diversity, based on which adaptive traffic splitting across multiple routing topologies is performed for dynamic load balancing. *AMPLE* system based on virtualized IGP routing topologies for dynamic traffic engineering. This adaptive TE aims to efficiently handle traffic dynamics at short time-scale such as hourly or even in minutes. This system does not require frequent and on-demand re-assignment of IGP link weights, thus minimizing the undesired transient loops and traffic instability. The proposed system consists of two complementary components: offline link weight optimization that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual routing topologies for long term operation through the optimized setting of link weights. Based on these diverse paths, adaptive traffic control performs intelligent traffic splitting across individual routing topologies in reaction to the monitored network dynamics at short timescale. *AMPLE* has a very high chance of achieving *near optimal* performance with only a small number of routing topologies [5].

A. OLWO:

First of all, a fundamental issue in OLWO (Offline Link Weight Optimization) is how to the definition of "path diversity" between PoPs for traffic engineering. Let's consider the following two scenarios of MT-IGP link weight configuration. In the first case, highly diverse paths (e.g. end-to-end disjoint ones) are available for some PoP level S-D pairs, while for some other pairs individual paths are completely overlapping with each other across all VRTs. In the second case, none of the S-D pairs have disjoint paths, but none of them are completely overlapping either. Obviously, in the first case if any "critical" link that is shared by all paths gets congested, its load cannot be alleviated through adjusting traffic splitting ratios at the associated sources, as their traffic will inevitably travel through this link no matter which VRT is used. Hence, our strategy targets the second scenario by achieving "balanced" path diversity across all S-D pairs. [7].

The network is dimensioned through offline link weight optimization using Multi-Topology IGPs for achieving maximum path diversity across multiple routing topologies. Based on this optimized MT-IGP configuration, an adaptive traffic engineering algorithm performs dynamic traffic splitting adjustment for balancing the load across multiple routing topologies in reaction to the monitored traffic dynamics. Such an approach is able to efficiently minimize the occurrence of network congestion without the necessity of frequently changing IGP link weights that may cause transient forwarding loops and routing instability [5].

The link weight optimization be performed frequently and reflect the shift in traffic demands. This scheme outperforms the local search approach adopted in [4] regarding the number of iterations needed to obtain a "good" link weight setting [6].

B. Network Traffic Monitoring:

Network monitoring is responsible for collecting up-to-date traffic conditions in real-time and plays an important role for supporting the ATC (Adaptive Traffic Control) operations [24]. Network traffic monitoring and measurement is increasingly regarded as an *essential function* for understanding and improving the performance and security of our cyber infrastructure. Network Traffic Monitor is a network analytic tool that examines local area network usage and provides a display of upload and downloads statistics. The main purpose of the application is monitoring the IP traffic between your local area network and Internet [23].

C. Adaptive Traffic Control:

The optimized MT-IGP link weights produced by OLWO, adaptive traffic control (ATC) can be invoked at short-time intervals during operation in order to re-optimize the utilization of network resources in reaction to traffic dynamics. The optimization objective of ATC is to minimize the maximum link utilization (MLU), which is defined as the highest utilization among all the links in the network. The rationale behind ATC is to perform

periodical and incremental traffic splitting ratio re-adjustments across VRTs based on traffic pattern "continuity" at short timescale, but without necessarily performing global routing re-optimization process from scratch every time [7].

VI. CONCLUSIONS

In this paper, we provide a survey of traffic engineering approaches that are aware of routing information gathered from previous scenarios and we come up with a survey of aware traffic engineering model. We now briefly describe how they work in unison as a whole TE system. First, optimized MT-IGP link weights are configured on top of the underlying MT-IGP platform and remain static until the next offline OWLO cycle. During this period, ATC plays the major role for adaptively re-balancing the load according to the traffic dynamics in short-time intervals. We include what are the routing algorithms are used in the IGP. Despite the fact that the connection-oriented approach targets at overcoming the constraints of the connectionless scheme, MPLS has not prevailed yet. Common intra-domain routing protocols (i.e. OSPF, IS-IS) have been and will continue to be deployed in large networks throughout the Internet. However, both approaches have not been stretched to its limits and there are many areas regarding the incorporation of history information in traffic engineering where further work can be contributed. For example, in most works described, the existence of monitoring information is simply assumed. We finally conclude with the formulation of a survey aware traffic engineering model.

ACKNOWLEDGEMENT

We would like to thank Prof. Dr. V. Palanisamy and my friends for sharing some of very useful and patient comments for different drafts of this paper.

REFERENCES:

[1] Bernard Fortz, Jennifer Rexford and Mikkel Thorup "Traffic Engineering with Traditional IP Routing Protocols."

[2] Ning wang, Kin hon ho, George pavlou, and Michael howarth, "An Overview of Routing Optimization for Internet Traffic Engineering."

[3] Mao-Bin Hu, Yong-Hong Wu, Rui Jiang, Qing-Song Wu, and Wen-Xu Wang. "Traffic Dynamics Based on Local Routing Strategy in a Weighted Scale-Free Network."

[4] Bernard Fortz, Mikkel Thorup. "Internet Traffic Engineering by Optimizing OSPF Weights." In: Proc. IEEE INFOCOM (2000).

[5] N. Wang, K-H. Ho and G. Pavlou, "Adaptive Multi-topology IGP Based Traffic Engineering with Near-Optimal Performance", Proc. IFIP Networking 2008.

[6] Paraskevi Fafali, Charalampos Patrikakis, Angelos Michalas, and Vassilios Loumos, "Internet Traffic Engineering: History monitoring information featuring routing algorithms."

[7] Ning Wang, Kin Hon Ho, George Pavlou, "AMPLE: An Adaptive Traffic Engineering System Based on Virtual Routing Topologies." IEEE communications Magazine March 2012.

[8] T. Li and H. Smit, "IS-IS extensions for traffic engineering." Work in progress, Internet Draft draftietf-isis-traffic-04.txt, August 2001.

[9] J. T. Moy. OSPF version 2. NetworkWorking Group, Request for Comments: 1247, http://search. ietf.org/rfc/rfc1247.txt, July 1991.

[10] R. Callon. Use of OSI IS-IS for routing in TCP/IP and dual environments. Network Working Group, Request for Comments: 1195, http://search.ietf.org/rfc/rfc1195.txt, December 1990.

[11] Cisco. Configuring OSPF, 1997. Documentation at http://www.cisco.com/univerc/cc/td/doc/product/software/ios113ed/113ed cr/np1 c/1cospf.htm.

[12] B. Fortz and M. Thorup, "Optimizing OSPF/IS-IS Weights in a Changing World", IEEE Journal on Selected Areas in Communications (JSAC), Vol. 20, No. 4, May 2002, pp. 756-767.

[13] D. O. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao, "Overview and principles of Internet traffic engineering," Internet Engineering Task Force, RFC 3272, May 2002.

[14] Constantino Lagoa, Hao Che and Bernardo A. Movsichoff, "Adaptive Control Algorithms for Decentralized Optimal Traffic Engineering in the Internet."

[15] M. Pi´oro and D. Medhi, *Routing, Flow, and Capacity Design in Commmunication and Computer Networks*. Morgan Kaufmann, 2004.

[16] J. Rexford, "Route optimization in IP networks," in *Handbook of Optimization in Telecommunications*, M. G. Resende and P. M. Pardalos, Eds. Springer Science+Business Media, 2006.

[17] Henrik Abrahamsson, Mats Bj¨orkman "Robust Traffic Engineering using L-balanced Weight-Settings in OSPF/IS-IS."

[18] A. Sridharan, R. Guerin, C. Diot, Achieving Near-Optimal Traffic Engineering Solutions for Current OSPF/IS-IS Networks, in: IEEE INFOCOM 2003, San Francisco, CA, 2003.

[19] Jun Wang, Yaling Yang, Li Xiao, Klara Nahrstedt, "Edge-based Traffic Engineering for OSPF Networks."

[20] D. Mitra and K. Ramakrishna, "A Case Study of Multiservice Multipriority Traffic Engineering Design," in *Proc. IEEE GLOBECOM*, December 1999.

[21] J. Rexford, "Route optimization in IP networks," in *Handbook of Optimization in Telecommunications*, Springer Science + Business Media, February 2006.

[22] J. He, M. Chiang, and J. Rexford." DATE: Distributed Adaptive Traffic Engineering." In *Proc. IEEE INFOCOMM*, volume 3, Barcelona, Catalunya, Spain, April, 2006.

[23] Radha S. Shirbhate, Pallavi A. Patil " Network Traffic Monitoring Using Intrusion Detection System."

[24] A. Asgari, R. Egan, P. Trimintzois and G. Pavlou, "Scalable Monitoring Support for Resource Management and Service Assurance," IEEE Network Magazine, Vol. 18, Issue 6, November 2004, pp. 6-18

[25] D. Awduche, Bijan Jabbari., "Internet traffic engineering using Multi-Protocol Label Switching (MPLS)", Computer Networks, vol. 40, September 2001.

[26] G. Apostolopoulos and et. al, "QoS Routing Mechanisms and OSPF extensions", IETF RFC 2676, August 1999.

[27] B. Fortz and M. Thorup, "Increasing Internet capacity using local search," Tech. Rep. IS-MG 2000/21, Universit´e Libre de Bruxelles, 2000. http://smg.ulb.ac.be/Preprints/Fortz00_21.html.

[28] Adrian C. smethurst, Michael F. Keohane, R. Waye Ogozaly, "Control plane security and traffic flow management ", US patent Issued on May 29, 2007.

[29] B.R. Hurley, C.J.R. seidl and W.F. Sewel, "A survey of Dynamic Routing Methods for circuit switched Traffic", IEEE communication magazine, September 1987.

[30] C. Villamizar, "OSPF Optimized Multipath", Internet draft, IETF, March 1998, draft-ietf-ospf-omp-oo.txt.

[31] D. Thaler and C.Hopps, "Multipath issues in unicast and multicast", Internet draft, IETF, April 1999, draft-thaler-multipath-o3.txt.

[32] C. Huitema, "Routing in the Internet", Prentice Hall, 1995.

[33] J. Moy, " OSPF Version 2", Internet rfc, IETF, May 1998, Technical Report.

[34] R. Guerin, Ariel Orda, "QoS based routing in networks", Infocom'97, 1997.

[35] Z. Wang, Crowcroft J., "Quality of Service Routing For Supporting Multimedia Communications", IEEE Journal on Selected Area of Communications, Volume 14, Issue 7, pp: 1228- 1234, September 1996.