Tree Routed Contingency Retrieval Mechanism for Virtual Private Networks

Mahalakshmi C, Ramaswamy M

Abstract*— *The paper embarks a retrieval methodology on the occurrence of a contingency to support a continuous transfer of data in the wired infrastructure of a virtual private network (VPN). The scheme envisages a new route between the source and destination in the architecture of a shared provider network to augment the disruption in the flow of traffic. It ensembles the minimum use of bandwidth in its formulation with a view to effectively avail the services and ensure a reliable delivery procedure. The philosophy bestows the creation of a viable alternate path in the form of a tree to carry forth the stream of data and acquire the best performance in terms of measurable indices. The results obtained through NS2 simulation illustrate the merits of the proposed strategy and emphasize its suitability for large scale transmission to meet the emerging needs.

***Index Terms*—Bandwidth, Performance metrics, Tree routing, VPN.**

I. INTRODUCTION

A virtual private network (VPN) offers its service as a replacement for networks constructed using private lines between geographically distant sites to enable communication through tunnels [1]. VPNs act like private networks constructed with dedicated lines by providing considerable quality of service (QoS) and security levels. It allows an efficient and flexible use of the common public network infrastructure in order that the resources can be adjusted to suit the varying traffic requirements of customers.

The QoS depends to a large extent on the available bandwidth in the links and the behaviour of the end points [2]. The usage of bandwidth is determined by the model which specifies the attributes and the behaviour of the end-points. Among the models which are proposed to specify a structure, the pipe and hose model [3-5] find prominence in provisioning the VPN. The process of provisioning is significant to ensure an uninterrupted transfer between customer sites.

A VPN provisions itself across the infrastructure of an either a public or third party network to realize dedicated connectivity among the users. It may not be required to deploy physical cables and consequently turns out to be economic and flexible in its operation. The VPNs enjoy resource guarantees through the services of a carrier but however are static and require complex service level agreements (SLAs).

The lack of guaranteed resource appears to emerge as a major factor in its inability to support the desired service demands that continue to queue upon them [6].

Though a variety of routing options are available still a tree based approach appears to be most suited for networks characterized by small-memory, low-power and low-complexity lightweight nodes. It offers its service for a node at different stages such as when its battery supply is below certain threshold. A tree can be constructed in the network and an appropriate scheme used to assign logical addresses to the network nodes.

The philosophy of routing the data in the form of a tree is extremely simple in light of the fact that a node forwards the packets through child nodes in the branches to its destination. It avoids elaborate exchange of the update sequences and the overheads that arise in the process of storing the actions in routing tables. The information traverses its path along the logical tree and in the event of the destination being a descendant node, the parent node is chosen as the next hop.

A hose model based VPN provisioning algorithm called MTRA has been suggested to provide customers with a secure and manageable communication environment. It has been found to process multiple set of requests and reduce the rejection ratio [7]. A bandwidth-delay constrained routing algorithm has been developed with the knowledge of ingress-egress node pairs in the network and minimizes the rejection rates for setting up on new paths [8]. Two fixed label routing algorithms have been evolved in order to minimize the stack depth and the number of labels used. The simulation results have been found to illustrate the applicability of multi-protocol label switching (MPLS) routing of large trees with few labels and small stack sizes [9]. A multi objective traffic engineering issue that includes both resource usage and link utilization has been solved as an optimization problem through the use of heuristic approach [10].

A packet scheduling scheme has been presented to control and maintain QoS parameters in VPNs within the confines of adaptive and programmable networks [11]. Two vital traffic engineering propositions have been investigated to maximize the number of VPNs established on the network backbone and find a set of resource efficient back paths in the hose model of VPN [12]. An approach for scalable routing of VPN has been designed and validated using BGP updates and router configurations from a large VPN provider [13]. A prototype architecture for VPN service has been found to allow guaranteed resources, customized control and support a highly dynamic scenario. A tailored search algorithm has been derived from the characteristic of desired VPN and shown that the complexity can be mitigated by a multitude of factors [14].

There is still an exquisite requirement to evolve alternate approaches with a primary focus to optimize on the use of bandwidth and extricate admirable QoS metrics.

II. PROBLEM DESCRIPTION

The primary objective echoes to arrive at a tree based retrieval strategy suitable for wired VPN with a view to maintain the transfer of data between the source and destination entities. The scheme orients to design a re- routing algorithm on the occurrence of a contingency and accomplish the packet transfer through the use of MPLS protocol in the

Manuscript received on November, 2012.

Mahalakshmi C, Department of Electrical Engineering, Annamalai University, Chidambaram, Tamil Nadu, India.

Ramaswamy M, Department of Electrical Engineering, Annamalai University, Chidambaram, Tamil Nadu, India.

minimum bandwidth path. It includes a methodology in the NS-2 platform to evaluate its performance in terms of its metrics and extradite its applicability in the practical world.

III. SYSTEM MODELING

The services of the VPN can be realized by creating the communication environment based on controlled segmentation of a shared network infrastructure. It enables a virtual topology on top of an existing platform and provides a cost effective method to emulate the characteristics of a private network. The process of provisioning involves maintaining a database of network nodes assigning the nodes to specific customer services, configuring them and activating the service.

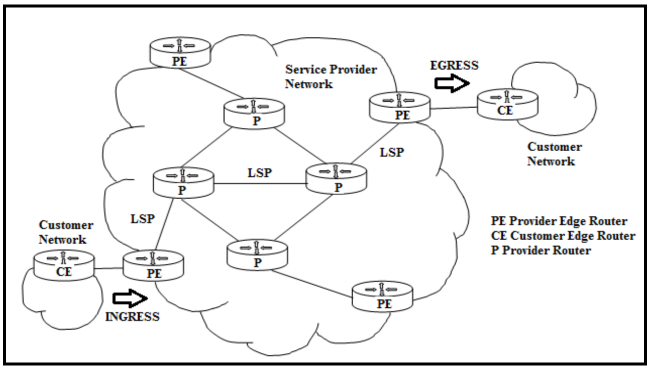

Figure 1: VPN Architecture

A typical architecture of the VPN shown in Fig. 1 includes customer edge (CE) devices, provider edge (PE) devices and routers on which the core of the provider network are responsible to carry forward the traffic within the frames formed by CE and PE. While the CE devices are associated with customer sites, the PE devices serve as a customer entry and exit points and are managed by the provider.

IV. PROPOSED SCHEME

The methodology forges to astutely provision the hose model of the VPN in order that it facilitates the minimum usage of bandwidth and extracts the desired QoS requirements. The hose architecture interfaces a VPN endpoint and the service provider's network and specifies the aggregate ingress b-(v) and egress parameter b+ (v) suitable for the chosen model to realize the flow of a continuous traffic [15].

The hose model explicitly allows a VPN endpoint to arbitrarily distribute its traffic to the other endpoints and enable it to dynamically change in tune with evolving needs over a period of time. However the flexibility may create potential congestion problems inside the VPN in light of the view as multiple VPN endpoint pairs may use the same links for their communications. Therefore it is highly desirable for every VPN endpoint pair to explore multiple alternative paths to conceive a load-balancing mechanism and uniformly distribute the traffic onto multiple paths.

The MPLS inherits a strong legacy from very early days to offer a means of transferring data through routers in VPNs. The fundamental concept underlying the theory of transfer augurs a clear separation of the control plane from the data plane in network switching elements. The functions of the data and control planes relate to label switching operations and network level coordination that be-hives routing and signaling to enable the movement of traffic in the environment.

The MPLS employs a router called label switching router (LSR) to provide explicit routing using label switched paths (LSPs) in the wired architecture of a VPN. It involves the assignment of the forward equivalence class (FEC) to the packet which is encoded into a label to serve as an identifier and forward the packets [16]. The packets are classified at the ingress and routed based on a combination of the information carried by the packets and local routing information maintained by the LSR. The LSR uses the label as the index to look up the forwarding table and process the packet in accordance with its entries. The scheme outlining the flow of packets with minimum usage of bandwidth is depicted in Fig. 2.

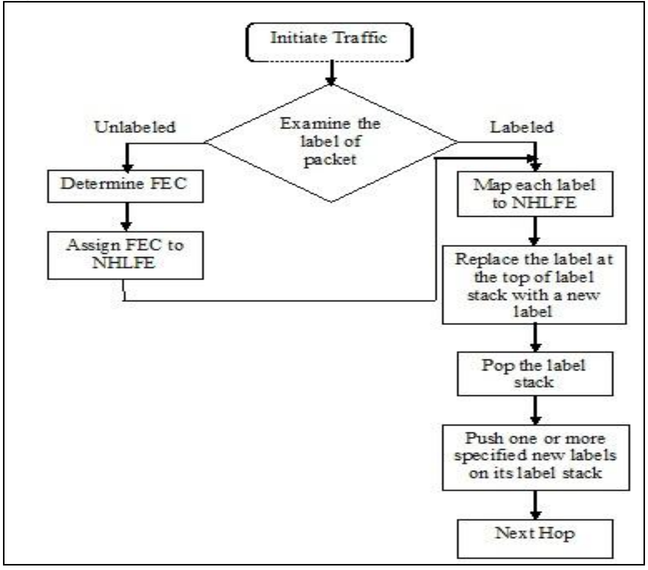
Initiate Traffic
Unlabeled
Examine the label of packet
Labeled
Determine FEC
Map each label to NHLFE
Assign FEC to NHLFE
Replace the label at the top of label stack with a new label
Pop the label stack
Push one or more specified new labels on its label stack
Next Hop

Figure 2: Flow Diagram of the Proposed Strategy

If a packet is received with an invalid label, it is discarded unless it is determined that it may not cause any harm on being forwarded. If the packet is explicitly routed, it can result in a loop and may not contain sufficient information to be forwarded correctly.

V. SIMULATION RESULTS

The formulation espouses transfer of data in a wired configuration of VPN depicted using NS-2 simulation schematic seen in Fig. 3 with fifty nodes over three paths connected in the form of a tree between the same source and destination nodes. The design attempts to forward the packets through the three paths sequentially on the occurrence of contingency in each of the paths to ensure the continuity in traffic. The strategy investigates the performance for similar time patterns with a data size of 1000 and the metrics measured in all the three paths.

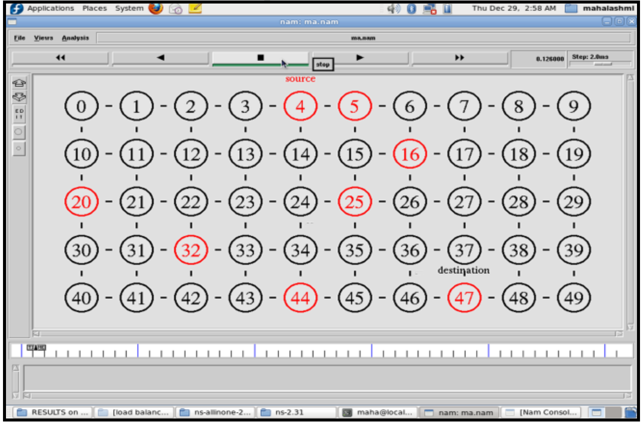

Figure 3: Network Topology

The performance graphs displayed through Figs. 4 and 7 explain the variation of the packets received, routing delay, packet loss, energy expended in the path that enjoys the usage of minimum bandwidth. The number of received packets, packets lost and use of energy to traverse the flow increase linearly as observed from Figs. 6, 7 and 8. Though the routing delay depicted in Fig. 9 appears to be initially high in view of start up, the algorithm tailors it to experience an exponential decrease in the stipulated time frame.

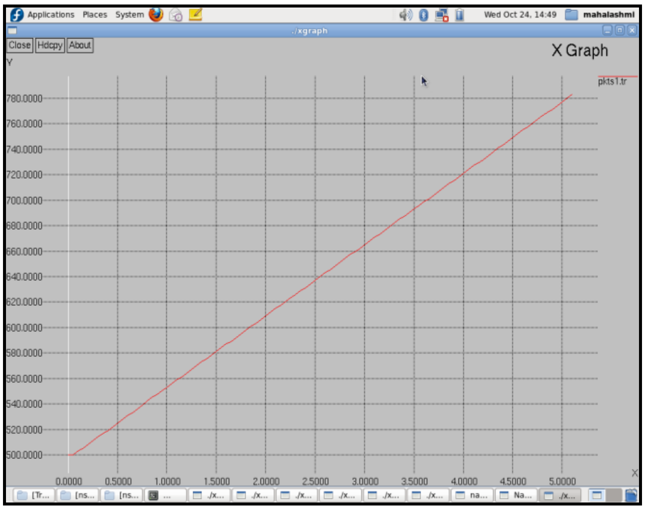

Figure 4: Packets Received vs. Time

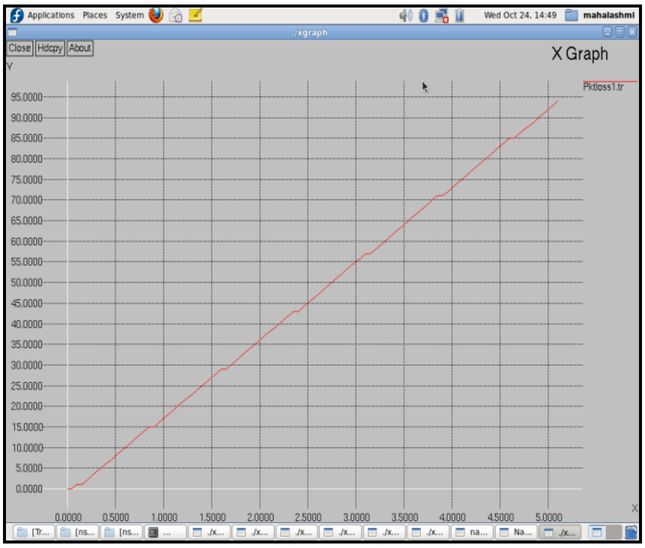

Figure 5: Packet Loss vs. Time

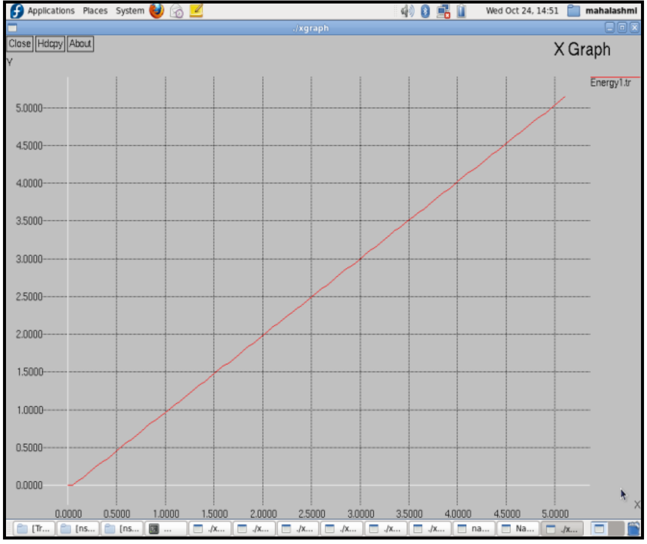

Figure 6: Energy vs. Time

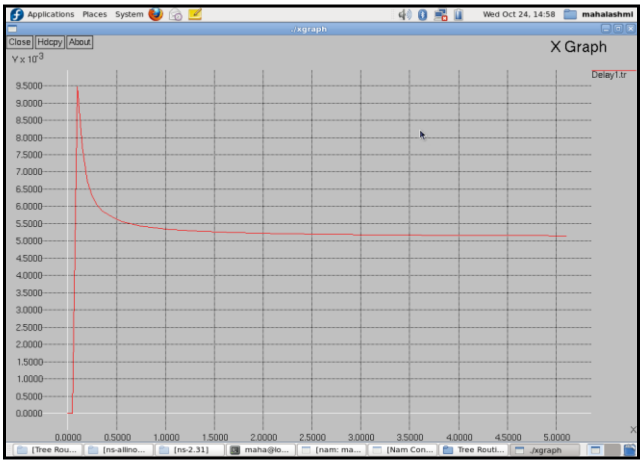

Figure 7: Routing Delay vs. Time

The entries in Table 1 compare the quantities that measure the strength of the proposed approach to validate the nuances of the design. It is evident that the indices acquire values in tune with the variations in bandwidth in the sense that the minimum bandwidth path extricates the highest values. However it follows that they do not widely fall apart and allow themselves to exploit the benefits of the scheme to archive a reliable delivery even in the case of an interruption in the stream.

Table 1. Performance Metrics

Paths	Bandwidth*10 ^{6}	Packets Received	Routing Delay * 10^{-3}	Packet Loss	Energy Expended* 10^{3}	Energy * Delay
1	0.479	785	9.5	92	5.1	48.9
2	0.576	620	13	140	5.4	70.2
3	0.608	535	22	188	6.1	134.2

The scheme is examined to explore the suitability of large scale data transmission through a systematic increase in the size of the packets and the performance measured in terms of its indices. The Figs. 8 and 9 display the increase in the number of packets received and associated fall in the transmission delay respectively over a viable operating range for the chosen architecture in the path which uses the minimum bandwidth, thus further highlighting the significance of the proposed routing methodology. However, there is an increase in the loss of packets and the energy expended as seen from Figs. 10 and 11.

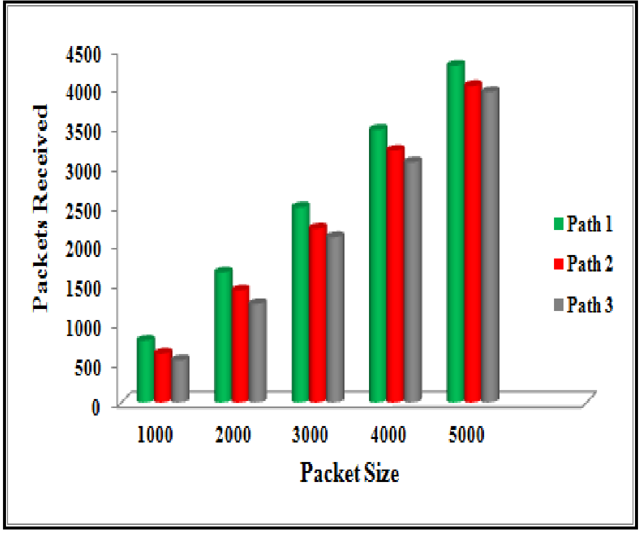

Figure 8: Packets Received vs. Packet Size

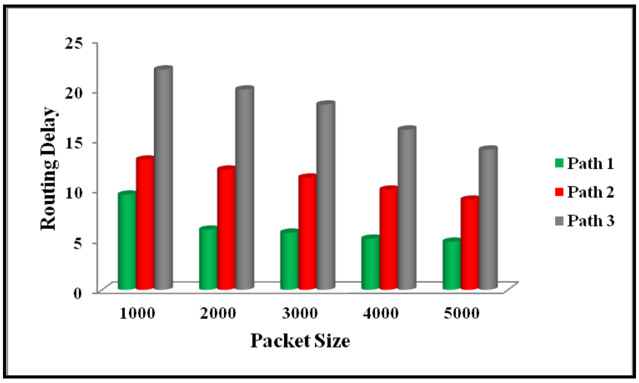

Figure 9: Routing Delay vs. Packet Size

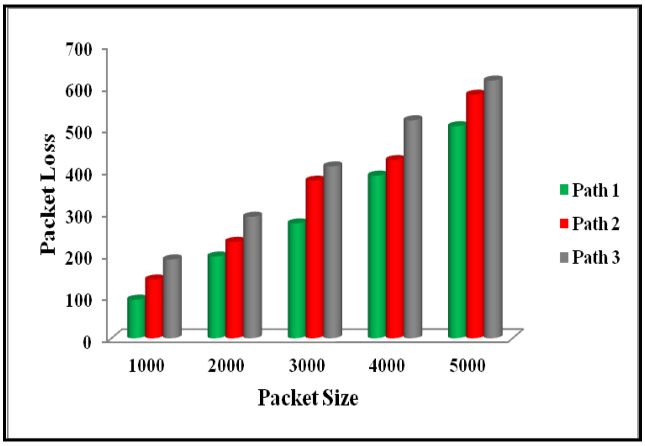

Figure 10: Packet Loss vs. Packet Size

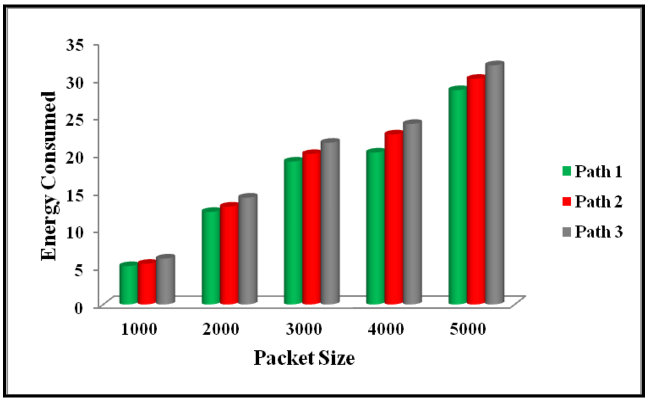

Figure 11: Energy Consumed vs. Packet Size

The network Packet Delivery Ratio (PDR) declines with increase in packet sizes due to the constraints in its load handling capability as observed from Fig. 12. The values of the different metrics project to realize the robustness of the scheme in the sense that the minimum bandwidth path continues to enjoy the best results over a wide range of data size.

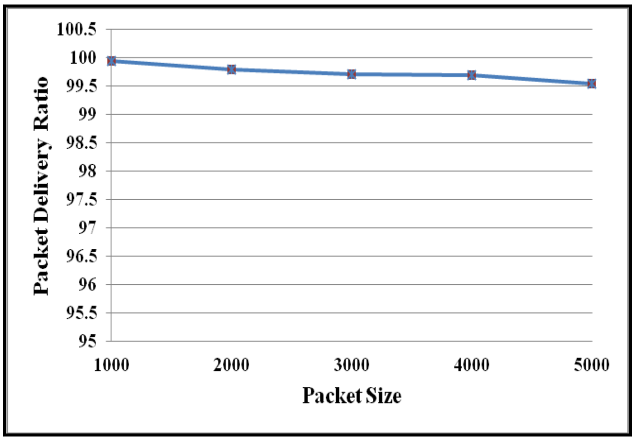

Figure 12: Packet Delivery Ratio vs. Packet Size

VI. CONCLUSION

A tree based routing strategy has been developed to transfer data between a source and destination in a wired VPN topology. The scheme has been designed to avail alternative routes on the occurrence of a contingency and ensure continuity in traffic. The NS2 simulation results have been found to increase the echelons of data transfer through this methodology. The performance indices have been found to project the merits of the algorithm in terms of bandwidth usage and support large scale data transmission. The viability of the proposed mechanism will enhance the plethora of options and assuage a reliable mode of communication in the automated world.

VII. ACKNOWLEDGMENT

The authors thank the authorities of Annamalai University for providing the necessary facilities in order to accomplish this piece of work.

REFERENCES

[1] N.G.Duffield, P.Goyal, A.Greenberg, P.Mishra, K.K.Ramakrishnan, and J.E. Van Der Merwe, 2002. “Resource Management with Hoses: Point-to- Cloud Services for Virtual Private Networks”, *IEEE/ACM Transactions on Networking*, 2002, pp. 679 – 692.

[2] Jian Chu and Chin-Tau Lea, “New Architecture and Algorithms for Fast Construction of Hose-Model VPNs”, *IEEE/ACM Transactions on Networking*, vol. 16, June 2008, pp.670-679.

[3] N. Duffield, P. Goyal and A. Greenberg, “A flexible model for resource management in virtual private networks,” in *ACM SIGCOMM*, 1999.

[4] A. Kumar, R. Rastogi, A. Silberschatz, and Bulent Yener, “Algorithms for Provisioning Virtual Private Networks in the Hose Model”, *IEEE/ACM Transactions on Networking*, August 2002, pp. 565 – 578,.

[5] A. Gupta, J.Kleinberg, A.Kumar, R.Rastogi, and B.Yener, “Provisioning a Virtual Private Network: A Network Design Problem for Multicommodity Flow,” *ACM Symp. Theory of Comp.*, 2001, pp. 389–398.

[6] Satish Raghunath and K. K. Ramakrishnan, “Resource Management for Virtual Private Networks”, *IEEE Communications Magazine*, April 2007, pp.38-44.

[7] Y. L. Liu, Y. S. Sun and M. C. Chen, “*MTRA*: An On-Line Hose-Model VPN Provisioning Algorithm”, Technical report TR-IIS-04-020, IIS, Academia Sinica, 2004.

[8] Yi Yang, L. Zhang, J. K. Muppala, and S. T. Chanson, “Bandwidth-delay Constrained Routing Algorithms”, *Computer Networks*, vol. 42, July 2003, pp. 503-520.

[9] A. Gupta, A. Kumar and R. Rastogi, “Exploring the Trade-off between Label Size and Stack Depth in MPLS Routing”, in *Proc.of IEEE INFOCOM*, 2003, pp. 544-554.

[10] Chun Tung Chou, “Traffic Engineering for MPLS-based Virtual Private Networks”, *Computer Networks*, vol. 44, March 2004, pp.319–333.

[11] R. Ravi and S. Radhakrishnan, “Provisioning QoS in Virtual Private Network using Dynamic Scheduling”, *Journal of Computer Science*, vol. 4, January 2008, pp. 1-5.

[12] Yu-Liang Liu, S.Yeali, Sun, and Meng Chang Chen, “Traffic Engineering for Hose-Model VPN Provisioning”, *IEEE Globecom*, vol. 2, 2005, pp.1080-1085.

[13] Zied Ben Houidi and Mickael Meulle, “A new VPN routing approach for large scale networks”, *18th Int. conf on Network Protocols*, 2010 pp.124-133.

[14] Rebecca Isaacs and Ian Leslie, “Support for Resource-Assured and Dynamic Virtual Private Networks”, *IEEE Journal on Selected Areas in Communications*, vol. 19, March 2001, pp. 460-472.

[15] Gee-Swee Poo, and Haibo Wang, “Multi-path routing versus tree routing for VPN bandwidth provisioning in the hose model”, *Journal of Computer Networks*, vol. 51, June 2007, pp. 1725–1743.

[16] Sahel Alouneh, Abdeslam En-nouaary, Anjali Agarwal, “A Multiple LSPs Approach to Secure Data in MPLS Networks”, *Journal of Networks*, vol. 2, August 2007, pp.51-58.

Mahalakshmi C obtained her Bachelor's Degree in Electrical and Electronics Engineering from Annamalai University in 2001 and Masters Degree in Power Systems Engineering from Annamalai University in 2005. She is currently working as an Assistant Professor in the Department of Electrical Engineering at Annamalai University. Her investigations find a place in a list of international journals. She is on her way to obtaining her Doctoral degree. Her areas of interest include Integrated Circuit Design, VLSI design, Communication Networks, Control Systems and Intelligent Control Strategies.

Ramaswamy M obtained his Bachelor's Degree in Electrical and Electronics engineering from Madurai Kamaraj University in 1985, Master's Degree in Power Systems Engineering in 1990 and Doctoral Degree in Electrical Engineering in 2007 at Annamalai University. He has a number of publications in National and International journals to his credit. His areas of interest include Power Electronics, Solid State Drives, Power System Voltage Stability Studies, HVDC Transmission, Fuzzy Control Techniques and Communication Networks.