Routing Methodology for Secure Transmission of data in Virtual Private Networks

Mahalakshmi C, Ramaswamy M

Abstract— The paper attempts to streamline the process of data transmission in a wired Virtual Private Network (VPN), with a view to foresee the occurrence of attacks and attach a sense of security to its travel. It translates the sequence of generation of keys in the process of routing and be-hives a sequence to wait for the related certificates before the transfer of data packets It avails the facilities in the hose architecture to relay the methodology in the minimum bandwidth path and ensure an uninterrupted data transfer over the leased lines in the private dedicated network. The design allows the stream of message to continue in alternative directions between the chosen source and destination in the event of occurrence of disruptions. The procedure springs up with computation of performance indices through Network Simulator-2 (NS-2) to exhibit the viability of the formulation for use in the practical world.

Index Terms— Bandwidth, Performance metrics, Security, Routing, VPN.

1 Introduction

THE virtual private networks (VPNs) appear to emerge as a significant interface in data communication technology and offer equivocal services to result in realistic cost savings and elaborate freedom of transfer [1]. It imbibes extraneous artefacts to combine the use of both private and public networks in its efforts to reach different segments of the society. The VPN incorporates software features to realize secure transmission of data through a process of encryption and signature authentication before the flow of the packets in the network [2]. It orients to afford comfort and inflict the administrative network facilities of large public networks for the benefit of users.

The pervasive risk associated in a VPN creates a need to foresee that it protects the services of a dedicated infrastructure. It may enter a public network and include remote nodes over which it experiences inadequate administrative control [3]. The VPN eclipses to suffer from breaches in isolation than the traditional private network in view of its circumspect interleaving nature and end up in an insecure service.

A threat analysis has been suggested and counter measures established for Wireless Sensor Networks [WSNs]. It has been designed using link layer encryption and authentication policies for defence against mote class outsiders [4]. A dynamic routing algorithm that randomizes delivery paths has been formulated for data transmission in WSN. The algorithm has been developed without introducing extra control messages and experiments reveal promising results [5]. The security related issues and challenges in WSN have been investigated. The possible security threats have been reviewed and the holistic view of robust security discussed [6]. An AODV based approach has been proposed to provide a secure WSN for changing the frequency of data transmission. The results have been found to display the decreased throughput from the malicious node with increase in the number of frequencies [7]. The policy relating to security algorithms in routing protocols for WSN has been outlined**.** The performance overhead on implementing these security protocols has been observed to be within acceptable limits [8]. The various security methods revolving around multi-homing VPN and their advantages have been reviewed. An advanced method of sending confidential data through a multi-homing VPN has been found to yield a reliable and secure mode of network transmission [9].

The primary feature of security includes the services of confidentiality, integrity, and assurance. The fundamental purpose ascribes to evade disclosure, prevent interference and minimize interruption in the scourge of transmitting sensitive information over public and privately managed networks. The focus necessitates formulating a routing pattern that interleaves issues of security in the process of transferring the data.

2 Problem Statement

The main theory encompasses the construction of a routing scheme that acquires an ability to ensure the secure transfer of data between defined source and destination points across multiple paths in the hose model of a VPN. The methodology focuses to initiate a method to generate keys and avail a sequence to return the flow of certificates to the source node and hitherto signify a prohibitive passage for the flow of packets.

The stream owes the role of a MPLS based formulation to arrive at the minimum bandwidth path and orchestrate to pull out admirable values for the performance indices in that path. It extends to devise alternative avenues on the occurrence of interruptions and allow the data to reach the user end through the same algorithm. The investigations in the Network Simulator-2 (NS-2) platform forecast its viability for large scale transmission and serve the needs of a pirated world.

3 System Modelling

The hose model appears to effectively support Quality of Service (QoS) requirements in the VPNs in the sense it enjoys

- *Mahalakshmi C is currently working as an Assistant Professor in Electrical Engineering in Annamalai University, Tamil Nadu, India. E-mail: maha_c2008@yahoo.com*
- *Co-Author Ramaswamy M is currently working as a Professor of Electrical Engineering in Annamalai University, Tamil Nadu, India. E-mail: aupowerstaff@gmail.com*

flexibility, ease of specification and can be realized with savings in capacity [10-11]. However, extra efforts become a usual practice to minimize the delay in the transfer of packets. The specifications of the VPN model include the VPN endpoints and their associated ingress and egress traffic outlay.

The structure in Fig. 1 configures the VPN tunnels to realize the related services through a dedicated topology. It comprises of customer edge (CE) devices and provider edge (PE) devices as the main constituents of the architecture. While the CE devices connect the various utilities in the customer site, the PE devices allow the process of data transfer [12].

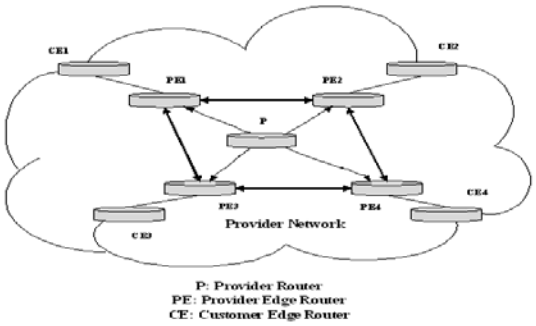

Fig. 1. Network model.

4 Proposed Methodology

The main objective bestows the generation of keys and archives a philosophy that returns certificates to the source node to relate the secure nature of the path. The procedure endeavours to formulate a mechanism that attempts to route the message through three different paths that connect a source and the chosen destination. It relays to forge the transfer with minimum use of bandwidth and extract the best QoS for that path. The strategy includes a facility to interleave contingencies and carry forth the packets in alternate streams and ensure the reach of the data to the receiver end.

The Multi-Protocol Label Switching (MPLS) relates to the identification of a specific path known as a Virtual Circuit (VC) by a label attached to each packet and eliminate the need to retrieve the address of the next node in the path. It facilitates the transfer of packets through the data link layer in the sense it simplifies the measures to extricate admirable QoS metrics using a connection-oriented switching approach.

The MPLS enables to provide re-routing mechanisms and permit an independent forwarding decision for each packet to be realized by the network layer routing algorithm. It involves two stages that initially form a set of Forwarding Equivalence Classes (FECs) by migrates to ensure that the packets received from a given neighbour and belong to a particular FEC follow the same path [13-16].

The procedure necessitates the FEC to send the label with the packet to its next hop and prevent the subsequent hops to analyse the network layer header in view of the fact that the label is used as an index into the table which specifies the next hop. The sequence replaces the old label and traverses the packet to its next hop with the new label.

The strategy outlined using the flow chart in Fig. 2 envisages formulating a secure routing methodology to forward the stream of data between a source and destination with minimum usage of bandwidth. The process initiates with a request from the source node to the VPN node for the generation of a certificate. The first significant step commences with the creation of a message digest algorithm from where it goes with the encryption scheme to generate a private key. The procedure at the other end favours the comparison of the digested message to create a public key that contains the identity of the source node. The VPN node thereafter replies with a certificate that contains the certificate's identity and request, signed by VPN with its private key, after which the sequence allows the flow of data.

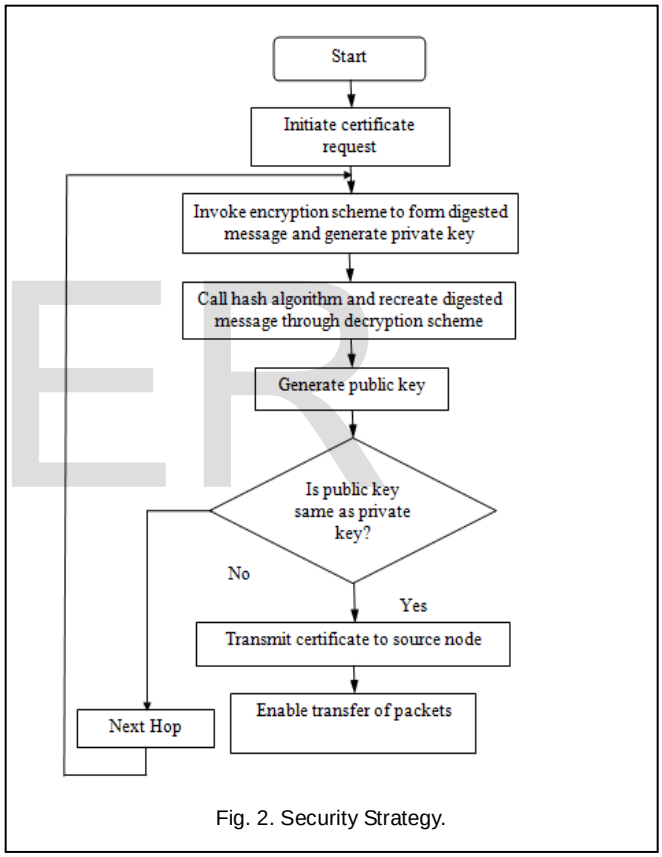

Fig. 2. Security Strategy.

5 Simulation Results

The approach avails a network with fifty nodes distributed in space over a size of 1000 m x 1000 m to implement the proposed methodology. The scheme realizes the minimum bandwidth path and transfers data between the chosen source and destination over a definite time frame. It introduces a contingency and equips with it a facility to continue the stream in the next minimum bandwidth path for another span of time and follows it in a similar fashion in the third path. The NS-2 figures depicting the data flow through the three paths is seen in Figs. 3 to 5.

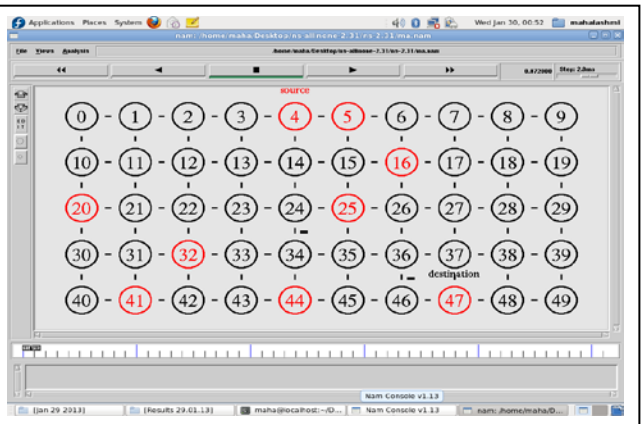

Fig. 3. Data Flow in Path 1.

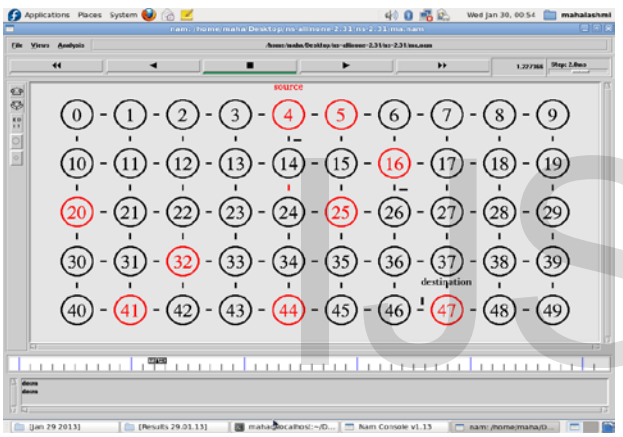

Fig. 4. Data Flow in Path 2.

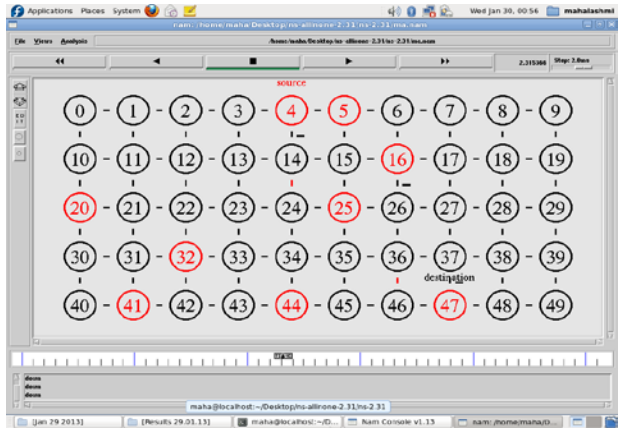

Fig. 5. Data Flow in Path 3.

The graph seen in Fig.6 relates the uniform variation of bandwidth used as a function of time in the streak to ensure the reliable passage of data. The Figs.7 through 10 exhibit the performance evaluated using NS-2 simulation in terms of the indices that include packets received, routing delay, packet loss and energy consumed in the process of data transmission through the first minimum bandwidth path over a predefined stretch of time. The measures experience a linear increase in their values except for the delay which appears to go through an exponential rise on account of the time involved to wait for the authenticated certificate from the VPN node.

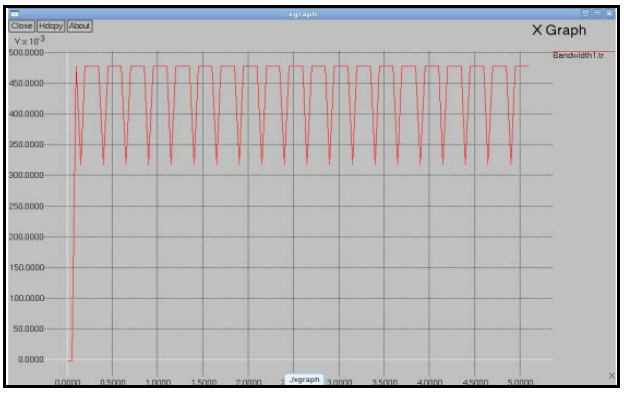

Fig. 6. Bandwidth vs Time.

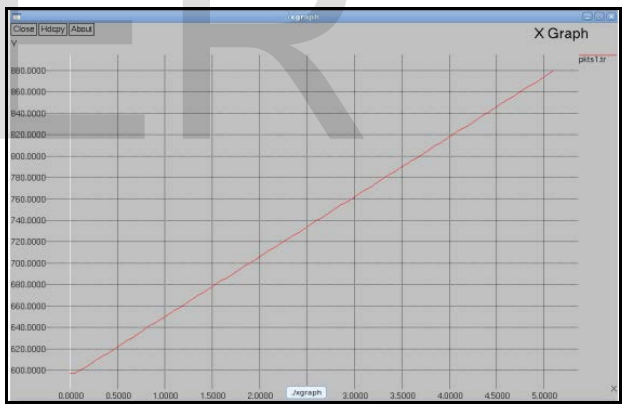

Fig. 7. Pactets Received vs Time.

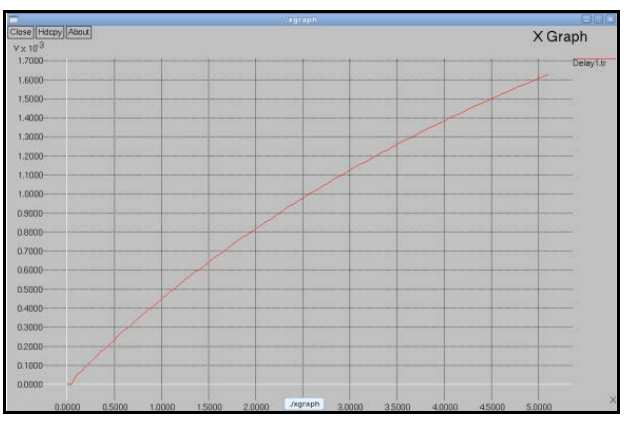

Fig. 8. Routing Delay vs Time.

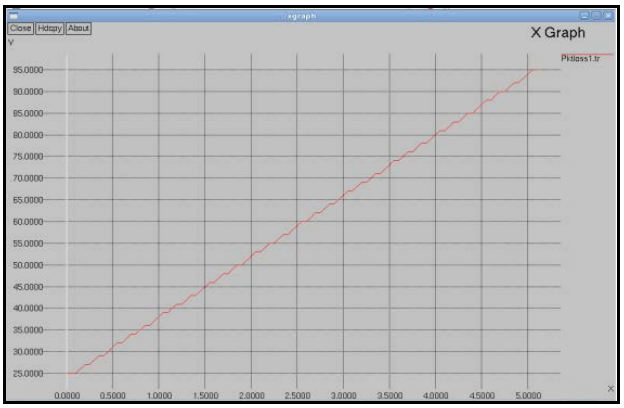

Fig. 9. Packet Loss vs Time.

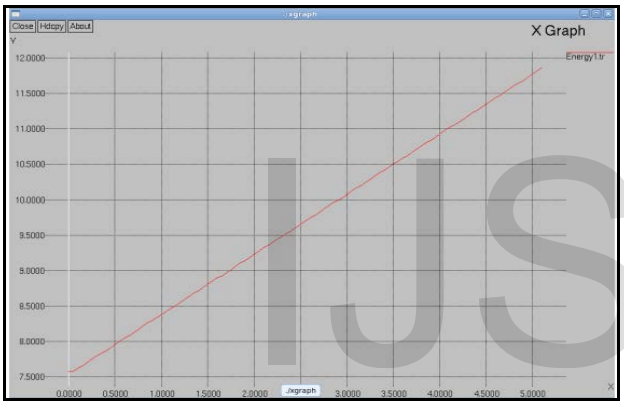

Fig. 10. Energy Expended vs Time.

The results in Table 1 reflect a comparative study for a packet size of 1000 bytes in three paths to epitomize the best performance for the minimum bandwidth path and validate the theory of the proposed formulation.

TABLE 1
PERFORMANCE METRICS

Paths	Band-width (Mbps)	Packets Received (Bytes)	Routing Delay x 10^{-3} (Sec)	Packet Loss (Bytes)	Energy Expended (J/Sec)
1	0.48	880	1.65	95	11.8
2	0.57	870	2.2	115	12.5
3	0.62	810	3.5	185	13.5

The strategy carries with it a facility to increase the size of the packets and elaborates the feasibility of the proposed approach for large scale transmission. The metrics except the delay enjoy an increase as observed from the bar charts in Figs. 11 through 13 and adds substance to the overall perspective of the algorithm. However the delay appears to decline across the higher range of data as seen from Fig. 14 further elaborating its merits.

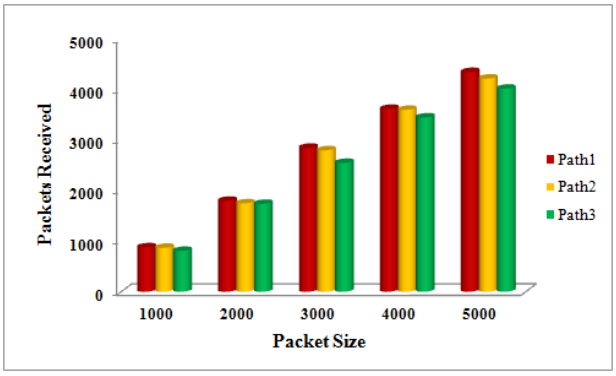

Fig. 11. Packets Received vs Packet size.

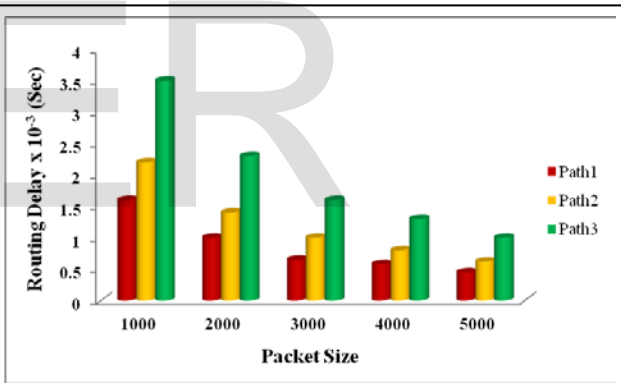

Fig. 12. Routing Delay vs Packet size.

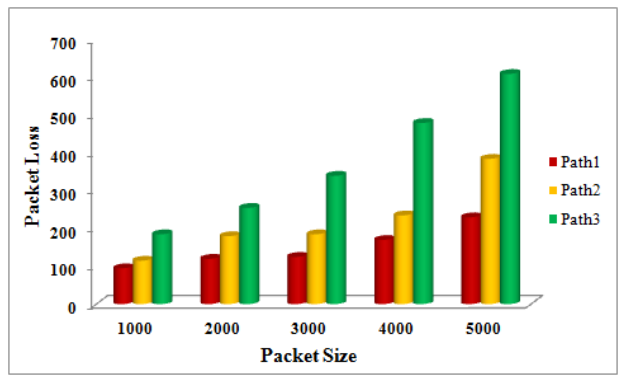

Fig. 13. Packet Loss vs Packet size.

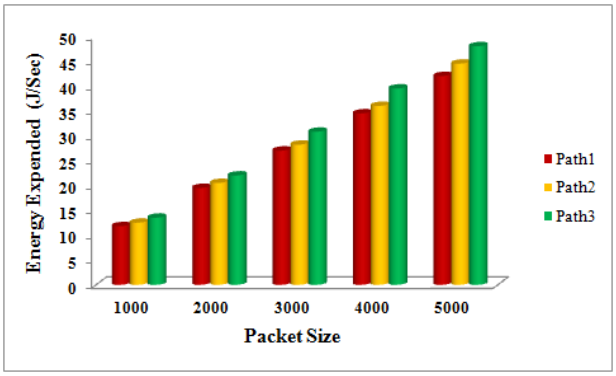

Fig. 14. Energy Expended vs Packet size.

There occurs a small decrease in the network Packet Delivery Ratio (PDR) in Fig. 15, calculated as a ratio of the number of packets received to the number of packets sent in a specific time frame in view of the issues that exhort its ability to handle the increasing sizes of the packets.

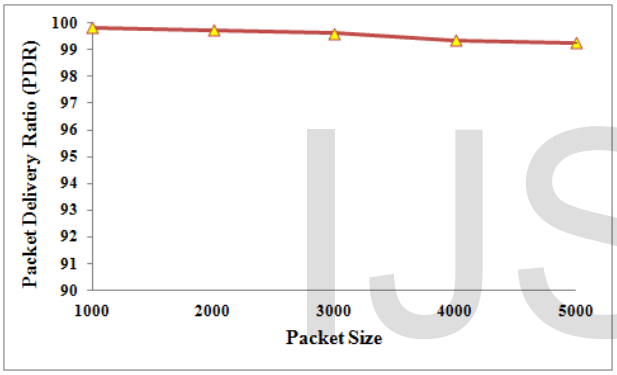

Fig. 15. Packet delivery ratio vs Packet size.

6 Conclusion

A MPLS based routing methodology has been articulated to transfer data in a secure wired VPN environment. The strategy has been designed through a series of steps that originate with the generation of a private key and verified using a public key to return a certificate to the source node. The performance evaluated on a NS-2 platform has been eschewed to project the minimum use of bandwidth for a safe passage of packets. The indices have been found to exhibit increasing levels of service in proportion to their bandwidths. The scheme has been laid to alleviate contingencies using alternative paths to route the data and accord a continuous transfer in the network. The multiplicity of paths along with the associated security will go a long way in ascribing new realms of data communication in VPN.

Acknowledgment

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

References

[1] Ishibashi, Ishisukha, Aida, and Kuribayashi, "Capacity dimensioning of VPN access links for elastic traffic in the hose model," *IEICE Trans. Communication*, vol. E87-B, no. 1, 2004.

[2] A.Thomas and G. Kelley, "Cost-effective vpn-based remote network connectivity over the internet", 2002.

[3] S.M. Krishna Ganesh, "VPN hose model provisioning using KDSVT," *Int. J. of Computer Application*, vol.2, no.2, pp.43-51, 2012.

[4] H.K. Kalita1 and A. Kar, "Wireless sensor network security analysis," *Int. J. of Next-Generation Networks*, vol.1, no.1, pp.1-10, 2009.

[5] G. Murali1, D. Pavan, V.V. Rajesh Reddy, and P.B. Kumar, "Dynamic routing with security considerations", *Int. J. of Computer Technology and Applications*, vol. 2, no.6, pp. 1790-1794, 2011.

[6] A.S.K. Pathan, H.W. Lee, and C. S. Hong, Security in wireless sensor networks: Issues and challenges," *The 8th International Conference on Advanced Communication Technology*, pp. 1043-1048, 2006.

[7] R. Haboub and M. Ouzzif, "Secure Routing in WSN," *Int. J. of Distributed and Parallel Systems*, vol.2, no.6, 2011, pp. 291-301.

[8] M. Sadeghi, F. Khosravi, K. Atefi, and M. Barati, "Security analysis of routing protocols in wireless sensor networks," *Int. J. of Computer Science Issues*, vol. 9, no.1, pp. 465-472, 2012.

[9] M. Sreedevi, and R. Seshadri, "Advanced security architecture for multi-homed virtual private networks," *American Journal of Scientific Research*, no. 22, pp.90-100, 2011.

[10] G. Veciana , S. Park, A. Sang, and S. Weber, "Routing and Provisioning VPNs based on hose traffic models and/or constraints," *Proceedings of 40th Annual Allerton Conference on Communication Control and Computing*, pp. 77-86, 2002.

[11] E. Oki and A. Iwaki, "Load-balanced IP routing scheme based on shortest paths in hose model," *IEEE Trans. on Communications*, vol. 58, no. 7, pp.2088-2096, 2010.

[12] D. Clercq and J. Paridaens, "Scalability implications of virtual private networks," *IEEE Communications Magazine*, vol.40, pp.151-157, 2002.

[13] M. Naraghi-Pour, and V. Desai, "Loop-free traffic engineering with path protection in MPLS VPNs," *Computer Networks*, vol. 52, no.12, pp.2360-2372, 2008.

[14] C. T. Chou, "Traffic engineering for mpls-based virtual private networks", *ComputerNetworks*, vol. 44, no.3, pp.319-333, 2004.

[15] K. Kar, M. Kodialam and T.V. Lakshman, "Minimum interference routing of bandwidth guaranteed tunnels with mpls traffic engineering applications", *IEEE J. of Selected Areas in Communications*, vol. 18, no. 12, pp. 2566-2579, 2000.

[16] S. Kulkarni, R.Sharma, and I. Mishra, "New bandwidth guaranteed qos routing algorithm for mpls networks," *J. of Emerging Trends in Computing and Information Sciences*, vol. 3, no.3, pp.384-389, 2012.