# DATA TRANSFER STRATEGY FOR MULTIPLE DESTINATION NODES IN VIRTUAL PRIVATE NETWORKS

[1]C. Mahalakshmi, [2]M.Ramaswamy
[1]Department of Electrical Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India
[2]Department of Electrical Engineering, Annamalai University, Annamalai Nagar, Tamil Nadu, India
E-Mail: maha_c2008@yahoo.com, aupowerstaff@gmail.com

## ABSTRACT

The paper attempts to design a data transfer scheme suitable for a host of receiver nodes in the wired infrastructure of a Virtual Private Network (VPN). The primary focus echoes a simultaneous data transfer strategy in the paths that inter connect a single source and multiple destinations in a wired VPN and offer a promising service similar to that of a dedicated private network. The methodology caters to extricate a suitable routing pattern to arrive at the preferred user across a service provider over specific time frames through an optimum use of bandwidth. It forges to acquire the best values of performance indices for that path which uses minimum bandwidth in each mission. The scheme be-hives a facility to re-route the data through an alternate path on the occurrence of a link failure to reach the desired destination. The performance of the routing mechanism simulated using a chosen network in the hose model serves to highlight the viability of the proposed approach to suit the befitting requirements in the field of data transfer.

**Keywords:** Data transfer, Virtual Private Network, bandwidth, performance indices, QoS.

## 1. INTRODUCTION

A Virtual Private Network (VPN) is a group of computer systems connected as a private network but communicates over a public network through leased lines. It is a logical network that is established on top of a physical entity to extract the behaviour of a dedicated environment with private lines [1]. A flexible model is significant in order to support a wide variety of customer needs in terms of capacity, network topology and communication patterns [2]. The providers of VPN services are required to address the QoS and security issues over a shared hose architecture that augur the specifications of ingress and egress traffic at each endpoint.

The creation of multiple paths between a single source and single destination node in a network serves to increase the reliability of data transmission. It splits the traffic and ensures that the source destination pair is not disconnected [3]. Though the maintenance costs and the associated complexity are its disadvantages, still the facility to optimally use the available bandwidth and avoid the intercepting interference inflicts its use for large scale traffic.

Provisioning the VPN involves providing a set of point-to-multipoint connections to accommodate the endpoints of the VPN. The service specification deliberately does not include details about the nature of traffic recognized by the nodes in a customer's network. However, these characteristics create an impact on the service level agreement (SLA) offered to the customer. Knowledge of the traffic matrix can depict the structure of interactions in the VPN [4].

The manners in which the VPN endpoints are actually connected evolve itself as a routing proposition. It revolves around the common goal of VPN operators to minimize the amount of bandwidth required for transferring the data in the network [5]. A strategy that recognizes and takes advantage of the distinct features of VPNs outperforms one that does not take these into account.

A capacity efficient and robust routing strategy called two phase routing has been described to allow preconfiguration of the VPN. It has been found to accommodate the permissible traffic pattern within the network natural ingress-egress capacity constraints [6]. Prototype architecture has been designed to guarantee resources, customized control and support a highly dynamic service in a VPN. A protocol has been formulated to adopt in the control plane to the process of resource revocation and thereby react gracefully to violation of service level agreements [7]. A multiobjective traffic engineering problem that incorporates both resource usage and link utilization in a VPN has been outlined. A heuristic solution has been evolved to solve this optimization problem to portray multiple classes of service for the VPN [8]. A load balancing algorithm has been articulated to suit multiple VPN entities. It has been found to serve both the service load requirements and the request business nodes load flow fluctuations. The results have been found to exhibit an improvement in the utilization rate [9]. A multiobjective multipath routing strategy has been orchestrated to solve the linear programme with maximum fraction of traffic on a path as a constraint. It has been found to reduce the bandwidth reservation on the most loaded link and thus alleviates the potential congestion problems in the service provider network [10]. An online routing algorithm has been presented for a VPN where routing requests arrive one by one without any a priori knowledge. It has been based on the idea that the new multicast route follows the path that does not interfere with the other critical routes [11]. Network architecture has been developed by adding a new VPN dynamically to overcome existing scalability problem in the hose model of the VPN. A linear programming formulation has been propounded to find the optimal route that in turn maximizes the amount of admissible traffic in the network [12]. A QoS model has been defined to evaluate the performance of signaling layer protocol in VPN. The scheme has been found to manage the resources according to a hose based provisioning mechanism. It has been found to modify the formats of the signaling messages to yield the desired performance [13].

Owing to the emergence of multiplicity nature of the traffic, there evinces a focus to explore viable multiplexed routing patterns between a common source and a number of destinations.

## 2. PROBLEM FORMULATION

The focus inflicts to evolve a routing scheme suitable to transfer data across a source and the host of destinations through different paths in a VPN. It assuages continuous traffic through the network and encompasses alternative streams in the event of contingencies. The MPLS based scheme outlays optimum use of bandwidth and enjoy tall values for the performance metrics in each path. It orients to investigate its performance through NS2 simulation and examine its suitability for practical applications.

## 3. SYSTEM MODELLING

A VPN provides a secure connection between a sender and the receiver over a public non-secure network such as the Internet. A VPN can transform the characteristics of a public non-secure network into those of a private secure network. The data transfer through VPN seems to be inexpensive owing to the fact that they reduce remote access costs by using public network resources. The cost benefits of VPN service appear to prompt corporations to move their data from private WANs to Internet based VPNs.

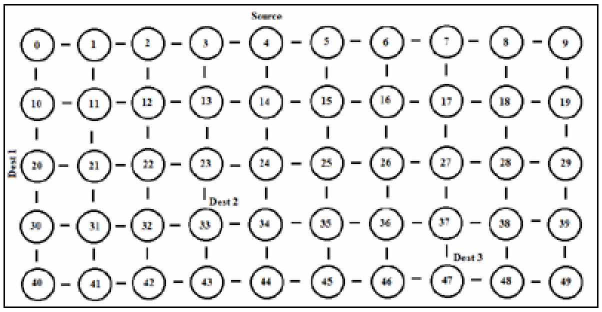

**Figure-1.** Network model.

The schematic of the chosen network in Figure-1 is seen to consist of fifty nodes distributed in space of size 1000 m x 1000 m. The internal architecture includes the customer edge (CE) devices to interconnect the different entities in each customer site and there after seeks the provider edge (PE) devices to facilitate the process of communication in the network [14]. The PE devices which reside in the service provider enable the VPN service by configuring VPN tunnels that in turn serve as a private line.

## 4. PROPOSED METHODOLOGY

In light of the fact that it is difficult to forecast the exact number of receiver nodes in a specific transmission path, there appears to be a challenge in ensuring the desired dynamic connectivity between the endpoints. The primary objective scatters to construct a mechanism with a view to transfer data from the source through a multiplicity of paths to reach the preferred destination among a set of receivers. It envisages realizing the desired Quality of Services (QoS) in the minimum bandwidth path and incorporating measures to create alternatives in the event of exigencies.

The focus of this paper is on using ‘hose models’ as a means to describe traffic demands on a VPN and characterizes the aggregate traffic in/out of a VPN’s end-points [15]. The model perpetuates a link into the network and embodies itself as an exquisite interface. It offers performance guarantees from a given endpoint to the set of all other endpoints in the VPN, and for the traffic to the given endpoint from the set of all other endpoints in the VPN [4].

The hose model first introduced in the context of VPNs by [16] enjoys a number of advantages that include ease of specification, flexibility, multiplexing gain and characterization. A traffic characterization is simple in the sense that it only needs to specify aggregates at ingress/egress points and explicitly determine the demands between all origin destination pairs. It not only provides the customer with a natural service model but significantly reduces the amount of data required. The other facility is that it attaches the required flexibility to the network to tune to the actual demands.

Though the hose model provides customers with simpler, more flexible SLAs, the model appears to present the provider with a more challenging problem in resource management. Under the conventional point-to-point model for specifying QoS, there is uncertainty about temporal variation in the traffic between the two points. It necessitates developing mechanisms with a view to cope with the complexities and allow providers to achieve significant multiplexing gains in the network [17].

The Multi-Protocol Label Switching (MPLS) avails a technique known as label switching to forward the data through the network [18]. It introduces a small, fixed-format label in front of each data packet and at each hop across the network; the packet is routed based on the value of the incoming interface and label. The path followed by the data in the network is defined by the transition in label values, as the label is swapped at each Label Switching Router (LSR). However since the mapping between labels is constant at each LSR, the path is determined by the initial label value. The scheme examines at the ingress point and decides for each packet the corresponding Label Switched Path (LSP) and accordingly assigns the label to it. It is based on factors such as the destination address, the QoS requirements and the current state of the network.

The set of all packets that are forwarded in the same way is known as a Forwarding Equivalence Class (FEC).

## 5. SIMULATION RESULTS

The mechanism is formulated to promote data transfer to three destination outfits in a network constituted with fifty nodes. The flow sequence explaining the simultaneous transmission of packets to the three receiver nodes is displayed in Figure-2. It is equipped to re-route the data through an alternate path on the occurrence of a link failure in one route at a time. The methodology seeks the use of NS-2 simulator to investigate its performance in the chosen paths that lead to three service points.

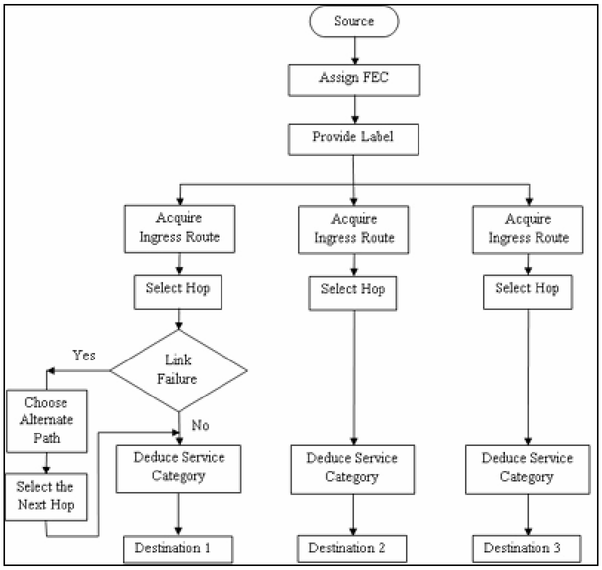

**Figure-2.** Flow algorithm of the proposed strategy.

The performance of the scheme is estimated using a set of indices namely packets received, routing delay, packet loss and energy expended to realize its effectiveness. The NS-2 graphs obtained during transfer of data of size 1000 in the path that uses minimum bandwidth to all the three destinations are portrayed using Figures 3 to 17. It is observed that except for the delay, the other metrics trace a linear increase with time before they reach their respective end points. Though it is initially high owing to start up, the routing delay begins to reduce and attain acceptable levels over the period of transmission. The Figures seen in 3 through 5 relate to the variation of bandwidth used as a function of time in the three cases, respectively.

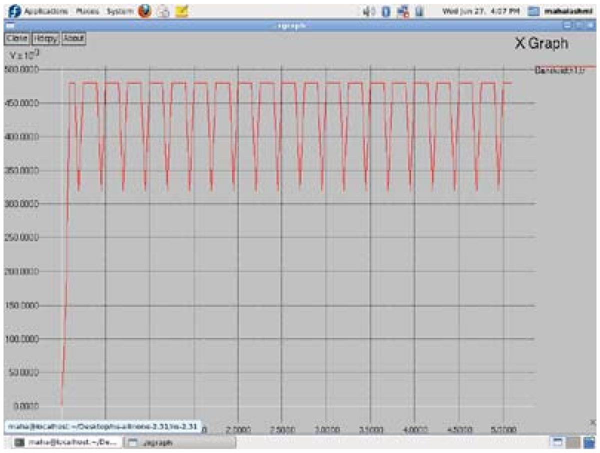

**Figure-3.** Bandwidth vs time (Destination 1).

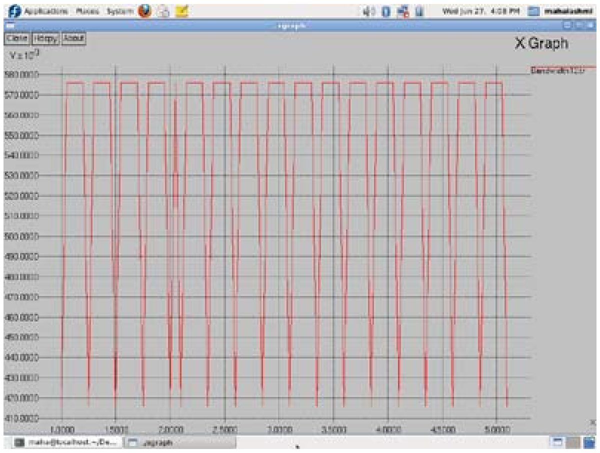

**Figure-4.** Bandwidth vs time (Destination 2).

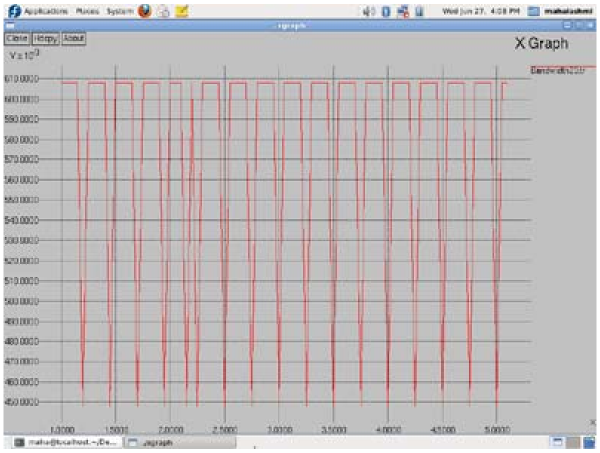

**Figure-5.** Bandwidth vs time (Destination 3).

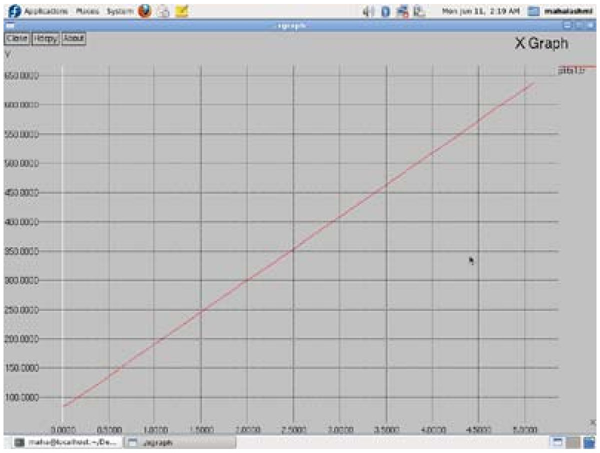

**Figure-6.** Packets received vs time (Destination 1).

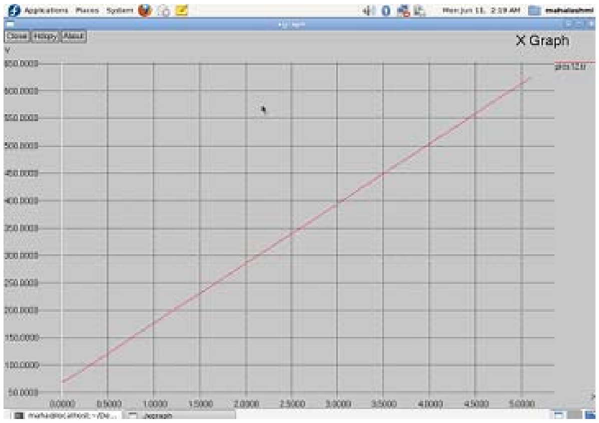

**Figure-7.** Packets received vs time (Destination 2).

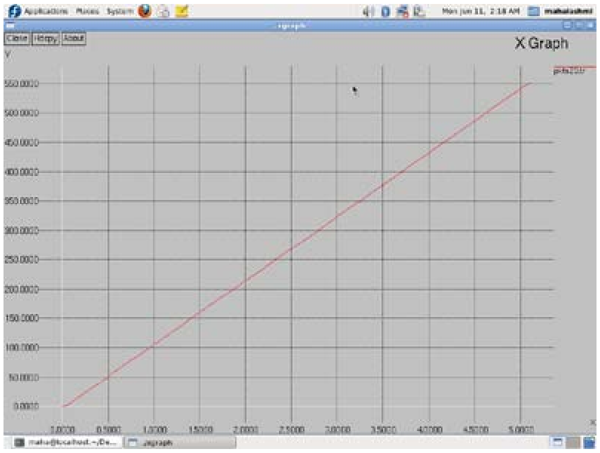

**Figure-8.** Packets received vs time (Destination 3).

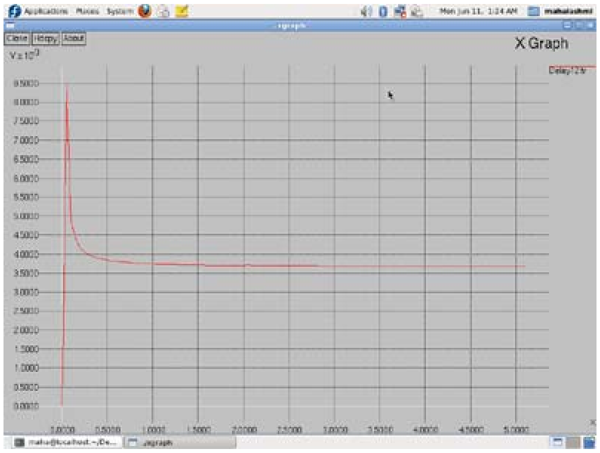

**Figure-9.** Routing delay vs time (Destination1).

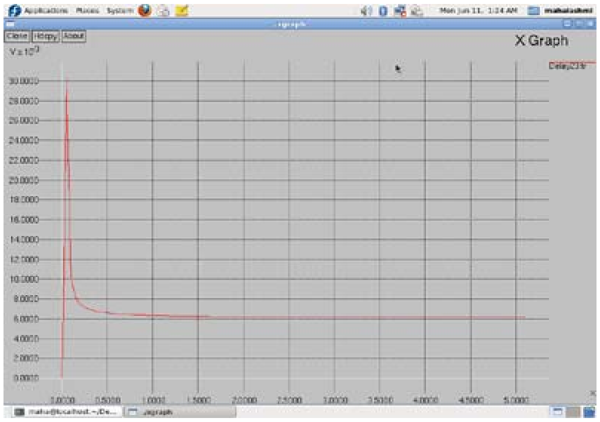

**Figure-10.** Routing delay vs time (Destination2).

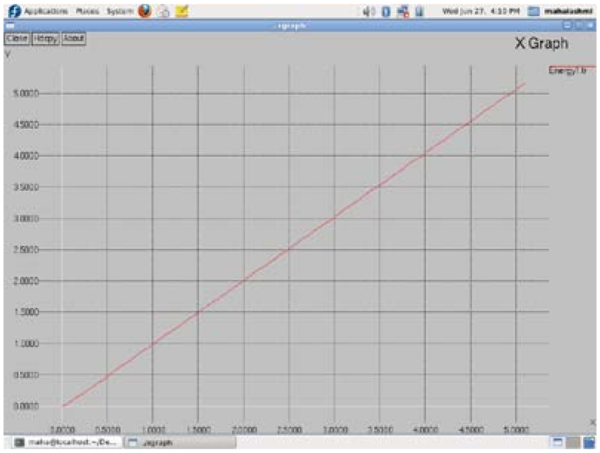

**Figure-11.** Routing delay vs time (Destination3).

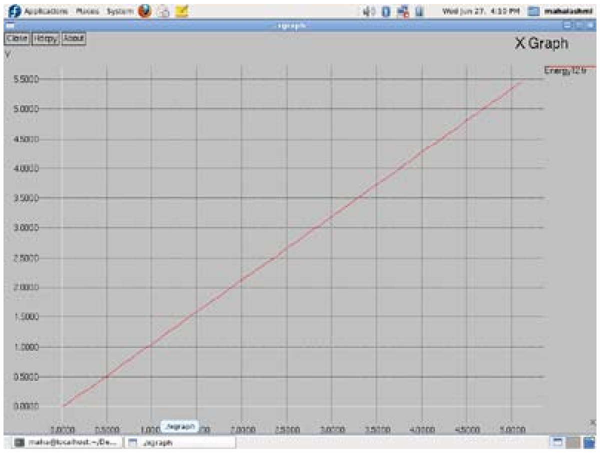

**Figure-12.** Energy vs time (Destination1).

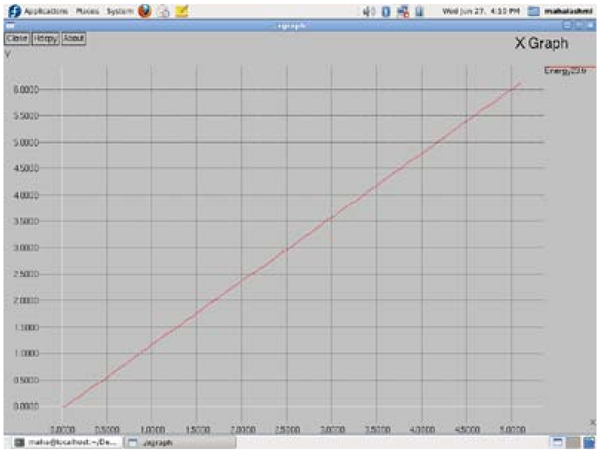

**Figure-13.** Energy vs time (Destination2).

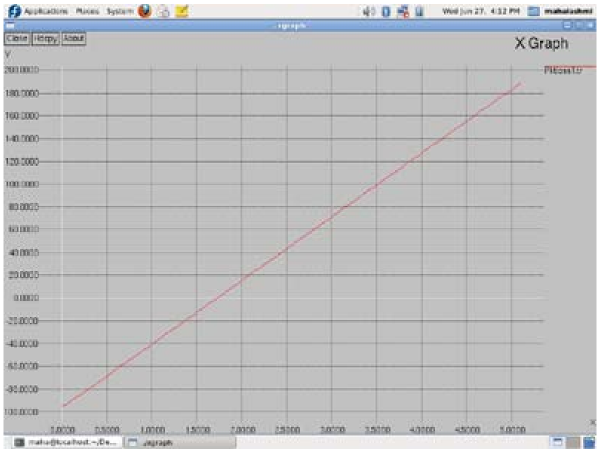

**Figure-14.** Energy vs time (Destination3).

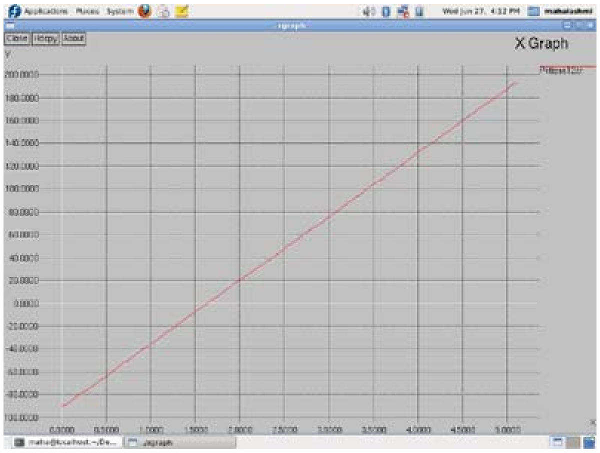

**Figure-15.** Packet loss vs time (Destination1).

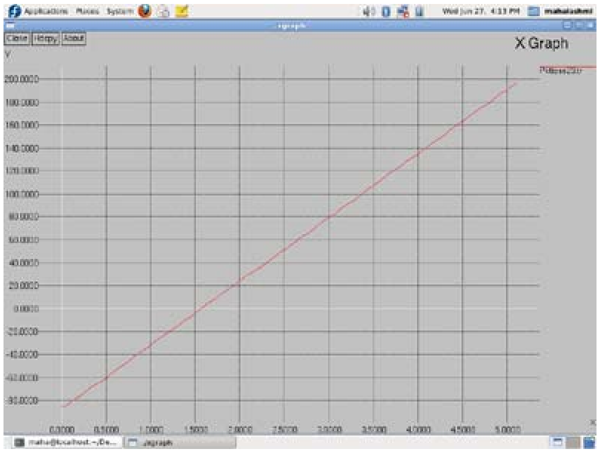

**Figure-16.** Packet loss vs time (Destination2).

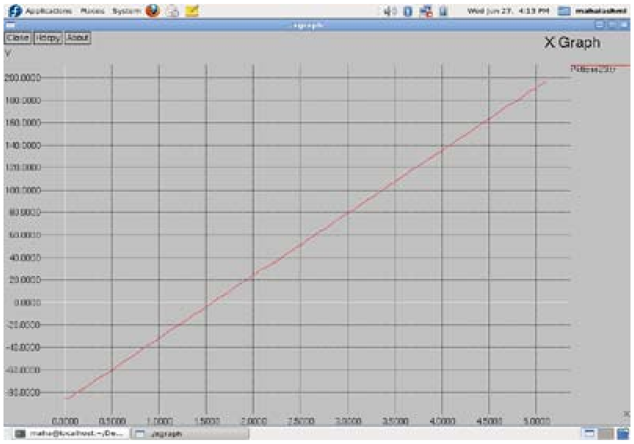

**Figure-17.** Packet loss vs time (Destination3).

The strategy inherits a procedure to carry the data in alternate routes in the event of link failures and ensure continuity in the process. The results acquired for a packet size of 512 following a contingency in each of the three paths one after the other that connect the source and the first destination are shown in Table-1. It follows that the algorithm allows the path that uses the minimum bandwidth to enjoy the best performance in terms of a higher number of packets received, lower usage of energy, packet loss and delay to accomplish the transfer.

TABLE 1
PERFORMANCE METRICS

| Paths | Bandwidth | Packets Received | Energy Consumed | Routing Delay x $10^{-3}$ | Packet Loss |
|---|---|---|---|---|---|
| 1 | 0.45 | 369 | 5.16 | 7.02 | 185 |
| 2 | 0.51 | 354 | 5.46 | 8.28 | 191 |
| 3 | 0.59 | 284 | 6.17 | 10.96 | 198 |

With a view to illustrate the ability of the scheme for large scale transmission, it is examined for varying packet sizes, the results of which are projected through bar charts in Figures 18 to 22. There is a consistent improvement to show a systematic rise in the number of packets received along with a marginal increase in the loss of packets and the energy required for routing the data. However the routing delay experiences a decline and thus adds weight to the merits of the proposed approach. The graph of network Packet Delivery Ratio (PDR) in Figure-22 remains almost constant and thereby establishes the supremacy of the formulation.

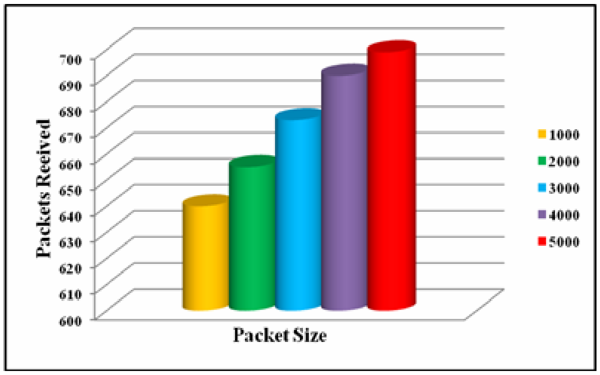

**Figure -18. Packets Received vs. Packet Size.**

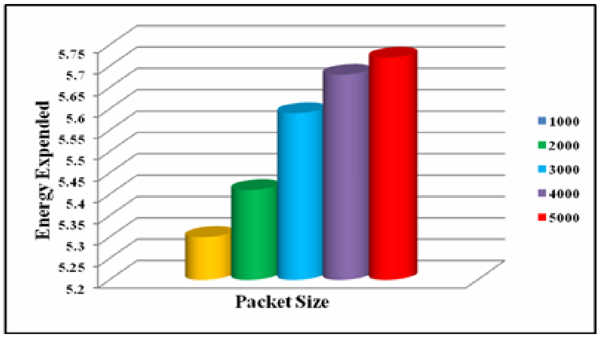

**Figure -19. Energy Expended vs. Packet Size.**

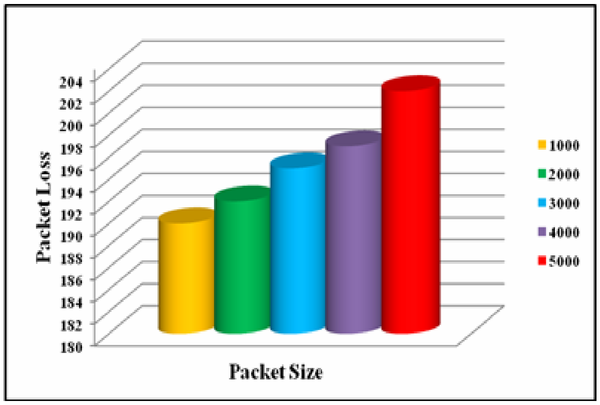

**Figure -21. Packet Loss vs. Packet Size.**

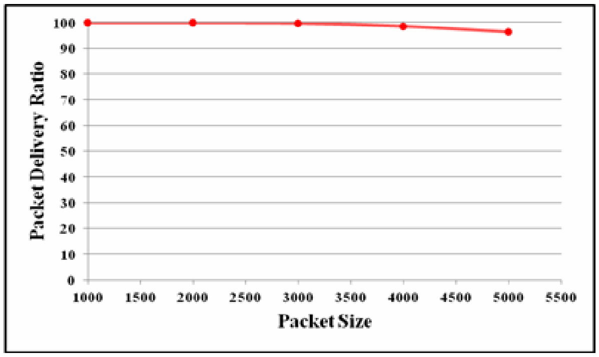

**Figure -22. Packet Delivery Ratio vs. Packet Size.**

## 6. CONCLUSIONS

A strategy to transmit data to a host of receiver stations has been proposed with a view to elaborate the potential for simultaneous transmission in the wired model of a VPN. The algorithm has been designed to ensure the minimum usage of bandwidth and still pull out acceptable values for the performance indices. The NS-2 based simulation results displayed for three destination nodes have been found to exhibit the capability of the routing procedure. The highlight of the methodology has been the creation of an alternate path in exigent states and allows an uninterrupted interchange between the source and preferred destination. It has been found to reach out to larger sized data with an admirable performance in terms of its metrics. The acclaimed merits have been centered to extend possible solutions for the increasing traffic and will enhance its scope in the emerging automated world.

## ACKNOWLEDGEMENT

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

## REFERENCES

[1] T. Erlebach and M.R uegg. 2004. Optimal bandwidth reservation in hose-model vpns with multi-path routing. In: Proc. of the 23rd Annual Joint Conference

of the IEEE Computer and Communications Societies INFOCOM. 4: 2275-2282.

[2] D. Wei and N. Ansari. 2004. Implementing fair bandwidth allocation schemes in hose-modelled VPN. In: IEEE Proceedings of Communications. 151: 521-528.

[3] Yuxin Mao. 2009. A feedback-based multipath approach for secure data collection in wireless sensor networks. Ubiquitous Computing and Communication J. 5: 27-32.

[4] S. Raghunath and K.K. Ramakrishnan. 2007. Resource management for virtual private networks. IEEE Communications Magazine. 45: 38-44.

[5] Tat Wing Chim, King-Shan Lui, Kwan L. Yeung and Chi Ping Wong. 2005. Routing algorithm for provisioning symmetric virtual private networks in the hose model. In: Proceeding of IEEE GLOBECOM. pp. 802-806.

[6] M. Kodialam, T. V. Lakshman, Sudipta Sengupta and Bell laboratories. 2007. Alcatel-lucent, Traffic-oblivious routing for guaranteed bandwidth performance. IEEE Communications Magazine. 45: 46-51.

[7] Rebecca Isaacs and Ian Leslie. 2001. Support for resource-assured and dynamic virtual private networks. IEEE J. on Selected Areas in Communications. 19: 460-472.

[8] Tung Chou. 2004. Traffic engineering for MPLS-based virtual private networks. Computer Networks. 44: 319-333.

[9] Zhe Zhang, Ling Gao, Hailin Xie and Qili Tao. 2010. Implementation of the load balancing for multiple VPN servers. In: proceeding of the Int. Conf. on Educational and Network Technology. pp. 147-150.

[10] H. Wang and G.-S. Poo. 2007. Load balancing in the provisioning of hose model virtual private networks with multi-path routing. IET Communications. 1: 684-692.

[11] Murali Kodialam, T. V. Lakshman and Sudipta Sengupta. 2003. Online multicast routing with bandwidth guarantees: A new approach using multicast network flow. IEEE/ACM Transactions on Networking. 11: 676-686.

[12] Jian Chu and Chin-Tau Lea. 2008. New architecture and algorithms for fast construction of hose- model VPNs. IEEE/ACM Transactions on Networking. 16: 670-679.

[13] Haesun Byun and Meejeong Lee. 2008. An NSIS based resource reservation protocol for hose model VPN service. International Conference on Advanced Communication Technology. pp. 207-211.

[14] De Clercq and J. Paridaens. 2002. Scalability implications of virtual private networks. IEEE Communications Magazine. 40: 151-157.

[15] Gustavo de Veciana, Sangkyu Park, Aimin Sang and Steven Weber. 2002. Routing and provisioning VPNs based on hose traffic models and/or constraints. In: Proceeding of 40th Annual Allerton Conference on Communication Control and Computing. pp. 7-86.

[16] N.G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K.K. Ramakrishnan and J. Merwe. 1999. A flexible model for resource management in virtual private networks. Proc. of ACM SIGCOMM. pp. 95-108.

[17] N.G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K. K. Ramakrishnan and J. van der Merive. 2002. Resource management with hoses: point-to-cloud services for virtual private networks. IEEE/ACM Transactions on Networking. pp. 679-692.

[18] O. Daniel, Awduche and Bijan Jabbari. 2002. Internet traffic Engineering using multi-protocol label switching. J. of Computer Networks. 40: 111-129.